



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2006-12

U.S. biodefense and homeland security toward detection and attribution

Bernett, Brian C.

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/2386>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. As such, it is in the public domain, and under the provisions of Title 17, United States Code, Section 105, is not copyrighted in the U.S.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**U.S. BIODEFENSE AND HOMELAND SECURITY:
TOWARD DETECTION AND ATTRIBUTION**

by

Brian C. Bennett

December 2006

Thesis Co-Advisors:

Peter R. Lavoy
Anne L. Clunan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE December 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: U.S. Biodefense and Homeland Security: Toward Detection and Attribution		5. FUNDING NUMBERS	
6. AUTHOR(S) Brian C. Bernett			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) <p>American leaders face tough decisions about the role of biodefense in homeland security. Debate centers on U.S. preparedness for biological attack, but few if any have adequately defined "preparedness." This thesis defines bioterrorism preparedness in terms of detection and attribution. Through case studies of the 1984 Rajneeshee cult and 2001 U.S. anthrax attacks, the thesis develops a notional model of biodefense that shows that nature of attack and the lethality or type of agent influence outbreak detection and biological weapons attribution. Because public health surveillance facilitates detection and interagency coordination facilitates attribution, there is a need to re-balance U.S. biodefense priorities by easing emphasis on current programs, and redirecting resources to simpler improvements in communication and organizational efficiency. Core limitations of the public health system that impede surveillance are discussed, and barriers between public health and law enforcement officials that hamper coordination are examined. Recommendations are provided to improve detection through better surveillance, and to enable attribution through better coordination and information sharing.</p>			
14. SUBJECT TERMS Biodefense, Bioterrorism, Biological Attack, Disease Outbreak Surveillance, Epidemiology, Detection, Attribution, Public Health, Forensic Epidemiology			15. NUMBER OF PAGES 142
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**U.S. BIODEFENSE AND HOMELAND SECURITY:
TOWARD DETECTION AND ATTRIBUTION**

Brian C. Bernett
Major, United States Air Force
B.S., United States Air Force Academy, 1991
M.S.H.S., Touro University International, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2006**

Author: Brian C. Bernett

Approved by: Peter R. Lavoy
Thesis Co-Advisor

Anne L. Clunan
Thesis Co-Advisor

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

American leaders face tough decisions about the role of biodefense in homeland security. Debate centers on U.S. preparedness for biological attack, but few if any have adequately defined “preparedness.” This thesis defines bioterrorism preparedness in terms of detection and attribution. Through case studies of the 1984 Rajneeshee cult and 2001 U.S. anthrax attacks, the thesis develops a notional model of biodefense that shows that nature of attack and the lethality or type of agent influence outbreak detection and biological weapons attribution. Because public health surveillance facilitates detection and interagency coordination facilitates attribution, there is a need to re-balance U.S. biodefense priorities by easing emphasis on current programs, and redirecting resources to simpler improvements in communication and organizational efficiency. Core limitations of the public health system that impede surveillance are discussed, and barriers between public health and law enforcement officials that hamper coordination are examined. Recommendations are provided to improve detection through better surveillance, and to enable attribution through better coordination and information sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION: A CASE FOR DETECTION AND ATTRIBUTION	1
A.	BACKGROUND	4
	1. Case Selection	4
	2. The Rajneeshees	5
	3. The Anthrax Attacks	6
B.	METHODOLOGY AND SOURCES	8
C.	THESIS ORGANIZATION	10
II.	THE RAJNEESHEE CULT BIOLOGICAL ATTACKS	13
A.	INTRODUCTION	13
B.	CASE SUMMARY	14
	1. Organization and Key Players	14
	2. Motivations	17
	3. Intentions	20
C.	NATURE OF ATTACK AND TARGET	22
D.	AGENT SELECTION AND ACQUISITION	25
E.	SURVEILLANCE AND EPIDEMIOLOGY	27
	1. Initial Reports	27
	2. First Response	28
	3. Epidemiological Investigation	29
	4. Suspicions and Initial Epidemiological Reports	30
F.	DETECTION AND ATTRIBUTION	31
G.	CASE FINDINGS	35
III.	THE U.S. ANTHRAX ATTACKS	39
A.	INTRODUCTION	39
B.	CASE SUMMARY	40
C.	NATURE OF ATTACK AND TARGET	45
D.	AGENT CONTROVERSY	47
	1. Anthrax and Its Potential Impact	47
	2. State versus Non-State Connection	48
	3. “Weaponized” versus “Pure”	52
E.	SURVEILLANCE AND EPIDEMIOLOGY	53
F.	DETECTION AND ATTRIBUTION	56
	1. “Anthrax Happens”	56
	2. Suspicions Rise	56
	3. Challenges of Coordination	57
G.	CASE FINDINGS	58
IV.	TOWARD DETECTION AND ATTRIBUTION	63
A.	CASE COMPARISON	64
B.	NOTIONAL MODEL OF BIODEFENSE	66
C.	BALANCING NATIONAL PRIORITIES	67

D.	DETECTION: SURVEILLANCE AND PUBLIC HEALTH LIMITATIONS.....	71
1.	Detection, Epidemiology, and Surveillance Defined in Terms of Public Health	71
2.	Composition and limits of the U.S. Public Health System	73
a.	<i>Limitation: Organizational Structure</i>	75
b.	<i>Limitation: Laboratory Capacity</i>	77
c.	<i>Limitation: The National Detection System</i>	79
3.	The National Biosurveillance Integration System (NBIS)	81
E.	ATTRIBUTION: COOPERATION AND COLLABORATIVE NETWORKS.....	83
1.	Managing Nature of Attack	83
2.	Roles in the Surveillance and Epidemiological Process.....	87
3.	Forensic Epidemiology and Existing Barriers to Coordination	88
V.	CONCLUSION	93
A.	THE FUTURE FRAMEWORK OF BIOTERRORISM	93
1.	Terrorists Are Managing Capabilities	94
2.	Mass Effects vs. Mass Destruction	95
3.	The Limits of Attribution for Dissuasion and Deterrence	97
B.	THE 1950s REVISITED.....	98
C.	RECOMMENDATIONS.....	102
1.	Improve Detection Through Better Surveillance.....	102
2.	Improve Attribution through Better Coordination and Information Sharing	105
3.	Conduct Realistic Training and Large-Scale Exercises	109
	LIST OF REFERENCES	113

LIST OF FIGURES

Figure 1.	“Comparison of State Biological WMD and Terrorist Biological Agent Development.” (From: Congressional Research Service Report, <i>Small-scale Terrorist Attacks Using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons</i> , May 20, 2004, CRS-15.)	22
Figure 2.	Rajneeshee Attack Epidemiological Curve. (From: Török et al., Figure 10.1 in <i>A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars</i> , 173.)	33
Figure 3.	2001 Anthrax Timeline. (From: <i>Toward a National Biodefense Strategy: Challenges and Opportunities</i> . Washington, D.C: Center for Counterproliferation Research, 2003, 10, http://www.ndu.edu/centercounter/CCR%202003.pdf (accessed December 20, 2005).)	40
Figure 4.	2001 Anthrax Contaminated Facilities. (From: <i>Observations and Lessons Learned from Anthrax Response: National Response Team Interim Report [Draft]—October to November, 2001</i> , 3, http://www.nrt.org/production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/A-80anthrax/\$File/ANTHRAX_Report_07_13_04.pdf?OpenElement (accessed November 26, 2005).)	41
Figure 5.	Surveillance facilitates detection.	67
Figure 6.	Interagency cooperation facilitates attribution.	67
Figure 7.	Epidemiological Clues That May Signal a Covert BW Attack. (From: <i>The Public Health Response</i> , Exhibit 2, 17.)	72
Figure 8.	The Connection between Detection and Response. (From: Wagner et al., <i>The Nation's Current Capacity</i> , 6.)	75
Figure 9.	The National Detection System (From: Wagner et al., <i>The Nation's Current Capacity</i> , Figure 3.1, 25.)	80
Figure 10.	Law Enforcement and Public Health Coordination by Nature of Event – Covert BW Attack. (From: <i>Collaboration between Public Health and Law Enforcement</i> .)	84
Figure 11.	Law Enforcement and Public Health Coordination by Nature of Event – Overt BW Attack. (From: <i>Collaboration between Public Health and Law Enforcement</i> .)	85

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	“Alleged Participants in Salmonella Contamination Activities.” (From: W. Seth Carus, Table 8.1 in <i>The Rajneeshees</i> (1984), 125.)	17
Table 2.	“Restaurant Contaminations Resulting in Illness in The Dalles, Oregon.” (From: W. Seth Carus, Table 8.2 in <i>The Rajneeshees</i> (1984), 132.)	28
Table 3.	The “Amerithrax” Medical Cases. (From: UCLA Department of Epidemiology, School of Public Health, http://www.ph.ucla.edu/epi/bioter/detect/antdetect_list.html (accessed March 1, 2006).)	42
Table 4.	Surveillance partners. (From: <i>The Public Health Response</i> , July 2001, 14.) ..	69
Table 5.	Response actors. (From: <i>The Public Health Response</i> , July 2001, 70.)	69

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ATCC	American Type Culture Collection
BARDA	Biomedical Advanced Research and Development Authority
BSL	Biosafety Level
BW	Biological Weapon(s)
BWC	Biological and Toxin Weapons Convention of 1972
CDC	Centers for Disease Control and Prevention
CONPLAN	Concept of Operations Plan
DHS	Department of Homeland Security
DOD	Department of Defense
EIS	Epidemic Intelligence Service
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
HHS	U.S. Department of Health and Human Services
HRSA	Health Resource and Services Administration
LRN	Laboratory Response Network
NBACC	National Biodefense Analysis and Countermeasures Center
NBIS	National Biosurveillance Integration System
RMC	Rajneesh Medical Corporation
SARS	Severe Acute Respiratory Syndrome
SNS	Strategic National Stockpile
TOPOFF	Top Officials Exercise
UNSCOM	United Nations Special Commission
USAMRIID	United States Army Medical Research Institute of Infectious Disease
USPS	United States Postal Service
WMD	Weapon(s) of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank several people whose help made this thesis possible. First, I express gratitude to my advisors, Professors Peter Lavoy and Anne Clunan. Professor Lavoy's class on counterproliferation sparked my interest in the topic and his direction kept an enormous project focused and manageable. Professor Clunan's expertise in organizational theory, and her research into building trusted networks for biological weapons attribution, greatly influenced much of my work. Special thanks go to Professor Craig Hooper of the Monterey Institute of International Studies (MIIS). Professor Hooper served as an additional reader and directed the study of the thesis' core section, Chapter IV. He provided important research material and fresh ideas based on his expertise as Scientist-in-Residence of the Center for Nonproliferation Studies. I am also grateful to classmate Chris Thompson who took time away from his work to analyze and critique mine.

I was able to participate in one workshop and a state-wide exercise that greatly contributed to the results. I would like to thank Professor Raymond Zilinskas of MIIS who organized the bioterrorism workshop I attended, and Cindy Lambdin of U.C. Berkeley's Center for Infectious Disease Preparedness, School of Public Health, who facilitated the table-top exercise. An interview was also conducted with Mrs. Lambdin during California's *Golden Guardian 2006* emergency response exercise. Additional thanks go to Dave Sullivan of San Francisco's Office of Emergency Services and Homeland Security. Mr. Sullivan led the simulation cell during *Golden Guardian* and allowed me to take part in the event.

Of course, the process of actually completing this thesis would have been impossible without the support of my family. I am indebted to and tremendously grateful for my wife Cynthia, whose support and encouragement saw me through. And to my sons Bradley, Adrian, and Ryan, who to me symbolize the future of America and serve as the reason to study Homeland Defense and Security.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION: A CASE FOR DETECTION AND ATTRIBUTION

Accessible, extremely destructive weapons that can be delivered by clandestine means represent a significant vulnerability, one which can be regarded as ‘small’ only in the sense that few aggressors have chosen to exploit it. We hope this threat continues to lie dormant, but believe it is imprudent to assume that it will.¹

American leaders face tough decisions about biodefense and its role in homeland security. Some debate U.S. preparedness for biological attack, but few if any have adequately defined “preparedness.” This thesis defines bioterrorism preparedness in terms of detection and attribution. It does this by analyzing the U.S. response in two cases: the Salmonella contamination of food by the Rajneesh cult in 1984, and epidemiological response to the anthrax attacks of 2001. Comparative case study will reveal the criticality of bioterrorism detection and attribution. These two requirements will then be compared to current U.S. biodefense programs to assess the extent to which the United States is adequately prepared. The results will show that medical surveillance, epidemiology, and the public health sector’s coordination with emergency services and law enforcement remain the weakest links. This work is not concerned with assessing the threat of bioterrorism—it proceeds on the premise that policymakers are concerned and will continue to fund U.S. programs. Moreover, it is not about bioterror mitigation or prevention—it presumes successful attacks are inevitable, even if only low-grade or small in scale. Rather, this thesis is about U.S. response and what defines good preparedness. The practical significance of its findings should permit policymakers to make informed decisions about interagency communication and networks at federal, state, and local levels of government. More importantly, the conceptual significance is that organizational structure and public-private partnerships may play a greater role in countering modern terrorism than previously thought.

At the time of this writing the World Health Organization reports the human-to-human spread of avian influenza H5N1 in Indonesia, U.S. Navy officials are testing

¹ Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, MA: MIT Press, 1998), xvii.

4,200 sailors and 1,200 visiting guests of the USS Ronald Regan for tuberculosis, and an outbreak of *E. Coli* from contaminated spinach is spreading across the United States. The first sparks fears of a global pandemic surpassing the 1918 worldwide influenza outbreak.² The second has U.S. officials considering whether to test high-ranking military officers from the People's Republic of China for tuberculosis.³ The third affects a \$180 million dollar-a-year crop and is costing spinach farmers \$50 to \$100 million dollars a month.⁴ Whether natural or deliberate, disease neither discriminates among populations nor respects international borders. It can have direct national security affects on troops and war-fighting readiness, or it can surreptitiously degrade a state's economy and critical infrastructure. While the events above have not been linked to terrorism per se, our ability to 1) rapidly detect outbreaks, and 2) characterize them as attacks and irrefutably attribute them to the perpetrators becomes nothing less than an essential core national capability. Investing in such capabilities produces synergistic returns. These include societal benefits from fighting emerging infectious disease by the private and public health sector, and national security benefits from bolstering U.S. dissuasion and deterrence postures against weapons of mass destruction (WMD) terrorism by the defense establishment.⁵

Finally, the tenuous link between money spent and potential future lives saved makes this issue important to national leaders. Debate continues to center on the low probability-high consequence nature of a biological attack compared to the large amounts

² Centers for Disease Control and Prevention, "Avian Influenza: Current Situation," <http://www.cdc.gov/flu/avian/outbreaks/current.htm> (accessed September 27, 2006).

³ Larry Shaughnessy, "Navy Tests Entire USS Reagan Crew for Tuberculosis," CNN.com, <http://www.cnn.com/CNN/Programs/situation.room/blog/2006/07/navy-tests-entire-uss-reagan-crew-for.html> (accessed September 27, 2006).

⁴ National Broadcast Corporation, "Feds: New Safety Plan Required Before Spinach Is Sold: E. Coli Source Discovered in Refrigerator," NBC11.com, <http://www.nbc11.com/news/9903292/detail.html> (accessed September 27, 2006) and Cable News Network, "FDA: E. Coli Linked to Natural Selection Foods," CNN.com, <http://www.cnn.com/2006/HEALTH/09/15/tainted.spinach.ap/index.html> (accessed September 27, 2006).

⁵ Michael Barletta, "Assessing Risks and Crafting Responses," *Center for Nonproliferation Studies Occasional Papers* 65, no. 8 (May 2002), <http://www.isn.ethz.ch/pubs/ph/details.cfm?v21=73370andid=14675> (accessed October 2, 2006), and The White House, *National Strategy for Combating Terrorism* (Washington, DC: The White House, September 2006), 14-15, <http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf> (accessed September 20, 2006).

invested in biodefense programs.⁶ With some \$30 billion spent in the four years since the 2001 anthrax attacks, and with the seeming lack of a biological threat since that time, the field is ripe for both scholarly and political debate.⁷ However, what if these expenditures and future budgeted biodefense dollars do little to actually improve preparedness? What if we learned the wrong lessons from previous events, and are over-weighting national biodefense programs and infrastructure development at the expense of uncomplicated training and interagency cooperation improvements? Projects BioShield, BioWatch, BioSense, and the National Biodefense Analysis and Countermeasures Center are the basis of today's publicly announced U.S. strategy.⁸ Yet consider that no amount of pre-positioned vaccine from BioShield and the Strategic National Stockpile (SNS) will help if state and local officials can not access, control, and distribute the medical countermeasures. BioWatch sensors are meaningless if those monitoring do not relay warnings to the people who need them most.⁹ Lastly, the BioSense national architecture will only be as good as the effectiveness of stakeholders using the system. Medical officials, physicians, pharmacies, and many others must embrace and use the network. While these consequence management capabilities are important, it also follows that "extraordinary measures are not necessary to develop a comprehensive terrorism health

⁶ Jessica Stern, "Terrorist Motivations and Unconventional Weapons," in *Planning the Unthinkable: How New Powers Will use Nuclear, Biological, and Chemical Weapons*, ed. Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz (Ithaca, NY: Cornell University Press, 2000), 203.

⁷ Milton Leitenberg cites an 18-fold increase in civilian biodefense expenditures in the past four fiscal years. He says the bioterror threat is over exaggerated, and that federal funds are inappropriately used when compared to the public health impact of other common diseases. Milton Leitenberg, "Assessing the Biological Weapons and Bioterrorism Threat," (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, December 2005), 4, 65.

⁸ These programs are covered in more detail in Chapter IV. BioShield deals with production and stockpiling of next generation medical countermeasures. BioWatch is a series of biological sensors strategically placed across the United States to detect agent release. BioSense is a web-based system combining laboratories, clinics, medical and public officials, BioWatch sensors, and other assets into a national architecture to increase situational awareness of possible disease outbreaks. The National Biodefense Analysis and Countermeasures Center is the first U.S. laboratory specifically focused on biodefense research.

⁹ Inconclusive tests prevented the Department of Homeland Security from notifying federal and local health agencies that sensors in the Washington, D.C. National Mall had detected tularemia. The Centers for Disease Control and Prevention did not learn of the biosensor readings for at least 72 hours, and it took five days for D.C.-area health agencies to receive the news. National Journal Group, "Inconclusive Test Results Cited in Delayed Tularemia Notification to Federal, Local Health Agencies," Global Security Newswire, http://www.nti.org/d_newswire/issues/2005/10/5/35653f39-93ee-416f-9540-a8cc79aaf652.html (accessed December 20, 2005).

surveillance and epidemiologic network.”¹⁰ The correct allocation of limited federal, state, and local resources makes this issue important. Today’s passive defense programs, which account for most all biodefense dollars, will be meaningless if the organizational challenges mentioned above are not addressed.

A. BACKGROUND

1. Case Selection

The 1984 Rajneesh cult and 2001 anthrax attacks cases are selected for four reasons. First, the cases are important in different ways. Rajneesh was the first documented biological weapons (BW) attack in the United States resulting in mass casualties, and for the first time challenged public health and law enforcement cooperation. The 2001 U.S. anthrax attacks, otherwise known as “Amerithrax,”¹¹ marked the first use of a lethal pathogen for terror on U.S. soil. Second, each demonstrates how the nature of BW attack (covert vs. overt) is directly related to an attacker’s objectives, their agent selection, and the ultimate outcomes. Third, the events occurred under very different national circumstances and levels of public awareness, yet highlighted similar gaps in our nation’s ability to manage biological crisis. Last and most importantly, these two cases are indicative of the types of attacks the United States may face in the future. “Chemical and biological weapons used in the past have not always been chosen for the highest potential fatalities, but rather for other reasons.”¹² The bioterror framework of the future suggests small-scale, specifically targeted attacks to create *mass effect* vs. mass casualties. What is more, these will likely be waged by non-state actors determined to escalate violence and climb the necessary technology-capability curve to achieve strategic objectives. It is for these reasons that the 1984 Rajneesh and 2001 Amerithrax cases are selected while other are omitted.

¹⁰ Department of Health and Human Services, *The Public Health Response to Biological and Chemical Terrorism: Interim Planning Guidance for State Public Health Officials* (Atlanta, GA: Centers for Disease Control and Prevention, July 2001), 15, <http://www.bt.cdc.gov/Documents/Planning/PlanningGuidance.PDF> (accessed March 28, 2006).

¹¹ FBI case name for the ongoing criminal investigation into the 2001 U.S. anthrax attacks. Federal Bureau of Investigation, “Amerithrax: The Search for Anthrax,” <http://www.fbi.gov/anthrax/searchant.htm> (accessed November 27, 2005).

¹² Dana A. Shea and Frank Gottron, *Small-Scale Terrorist Attacks using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons* (Washington, D.C.: Congressional Research Service, May 20, 2004), i, <http://fpc.state.gov/documents/organization/33629.pdf> (accessed March 28, 2006).

2. The Rajneeshees

In 1984 the Rajneesh cult succeeded with the first documented bioterror incident in the United States. Until then, there had been 222 bioterror related incidents in the United States with only 24 being confirmed attacks. Of these, only the Rajneesh attack had resulted in mass casualties.¹³ The group conspired to unseat the local government of The Dalles, Oregon, by using *Salmonella typhimurium* to sicken voters and swing an upcoming election.¹⁴ The cult ordered and received bacterial disks from a Seattle medical supply company. Key members used a laboratory with an incubator and freeze dryer to culture what they called salmonella “salsa.”¹⁵ Beginning August 29, 1984, several Rajneeshees sprinkled the salsa “in personal drinking glasses, on doorknobs and urinal handles, on produce at the local supermarket, and on salad bars in eleven restaurants.”¹⁶ Their attack hospitalized 45, caused 751 to fall ill, and would serve as a historical benchmark of bioterrorism in the United States.

By late 1984 local public health officials concluded the outbreaks were accidentally caused by contaminated food handlers. It took only four days for local health care providers to identify *Salmonella typhimurium* as the source, but over a year for the Centers for Disease Control and Prevention (CDC) to file its final report and confirm that a single strain had caused all of the illnesses.¹⁷ The attacks went unattributed to bioterrorism until the cult fractured from within. In September 1985, the Rajneesh leader publicly accused others in the group of mismanagement and

¹³ Henry S. Parker, “Agricultural Bioterrorism: A Federal Strategy to Meet the Threat,” *McNair Paper* 65 (March 2002), 19, <http://www.au.af.mil/au/awc/awcgate/ndu/mcnair65.pdf> (accessed November 26, 2005).

¹⁴ Raymond A. Zilinskas, “Biocriminality and Bioterrorism: Assessing the Threats,” (Monterey Institute of International Studies, November 4, 2005), slides 25-29. Presentation given as part of Workshop 548, “Simulating a Deliberately Caused Foodborne Disease Outbreak Using the Table-top Exercise (TTX),” held at Monterey Institute of International Studies on 4 and 12 November, 2005.

¹⁵ Per Anderson, “The Rajneeshee Cult,” Passagen, <http://hem.passagen.se/jan.olofsson/biowarfare/history/rajneeshee.html> (accessed November 26, 2005).

¹⁶ Ibid.

¹⁷ Ibid.

poisonings.¹⁸ The Oregon Attorney General directed a joint task force between state police and the Federal Bureau of Investigation (FBI) that eventually led to the group's demise.

A combination of slow medical surveillance and poor law enforcement integration with the public health system suggests a lack of preparedness for this biological attack. The Rajneesh cult event was the first case to reveal the vulnerability of civilian populations to chemical, biological, radiological, or nuclear terrorism.¹⁹ Likewise, it changed public health and law enforcement perspectives regarding bioterrorism, but did little to advance genuine biodefense preparedness in the United States.

3. The Anthrax Attacks

The use of *Bacillus anthracis* through the U.S. Postal System marks the first biological attack on American soil in the twenty-first century.²⁰ The attacks resulted in 11 inhalational cases and five deaths, and the terrorist(s) remain at large today.²¹ A detailed review shows the United States was far from having a comprehensive national biodefense strategy despite lessons learned from the 1984 Rajneesh attacks and reasonable attempts to improve preparedness. This event was a wake-up call to Americans and policymakers alike, and served as a tipping point in national security policy that resulted in many of the biodefense initiatives underway today.

High demand for sample testing met with only modest capability during the crisis.²² The Department of Defense provided operational support through the United States Army Medical Research Institute of Infectious Disease (USAMRIID). Originally designed to only assist with ten samples a month during an emergency, USAMRIID received more than 700 samples in a single day during the anthrax investigation, and

¹⁸ Zilinskas, *Biocriminality and Bioterrorism*, November 4, 2005.

¹⁹ Jonathan B. Tucker, "Historical Trends Related to Bioterrorism: An Empirical Analysis," *Emerging Infectious Disease* 5, no. 4 (1999), 498, <http://www.cdc.gov/ncidod/EID/vol5no4/pdf/tucker.pdf> (accessed November 26, 2005).

²⁰ National Defense University, *Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks* (Washington, D.C.: Center for Counterproliferation Research, November 2002), 2, http://www.ndu.edu/centercounter/prolif_publications.htm (accessed November 26, 2005).

²¹ Barry S. Levy and Victor W. Sidel, *Terrorism and Public Health: A Balanced Approach to Strengthening Systems and Protecting People* (New York: Oxford University Press, 2003), 105.

²² National Defense University, *Anthrax in America*, 6.

surged to process more than 14,000 specimens during the crisis.²³ Deficiencies were identified in information technology. The General Accounting Office (GAO) found six key federal agencies involved in bioterrorism preparedness and response, with some 70 systems in several information technology categories associated with public health emergency support.²⁴ The main areas included detection, surveillance, communication, and support technologies. The report found interoperability to be a major problem. CDC procedures were also reviewed, and questions were raised about oversight effectiveness of the Select Agent Transfer Program. At the time, the CDC's Laboratory Registration/Select Agent Transfer Program safeguarded and maintained positive control of 42 designated bacteria, viruses, and toxins. A November 2002 GAO report found the CDC's oversight left room for improvement.²⁵

Awareness that infections stemmed from a deliberate act turned what started out as a public health response into a law enforcement investigation. Environmental Protection Agency (EPA) and FBI hazardous material teams worked side-by-side, searching 280 barrels containing 635 bags of quarantined mail that had been seized as evidence.²⁶ Specific protocols were created on-the-fly to satisfy the needs of both federal agencies—to contain and clean up for the EPA, and to find and protect evidence leading to a criminal conviction for the FBI.²⁷ On the whole, hospital physicians and staffs responded well. However, some misdiagnosis and the resultant unnecessary deaths stand out as failures among successes with regard to surveillance and epidemiology. Ultimately, the implications of this case for U.S. biodefense preparedness are twofold. It identifies the need for improved interagency cooperation to enhance response, and

²³ National Defense University, *Toward a National Biodefense Strategy: Challenges and Opportunities* (Washington, D.C: Center for Counterproliferation Research, 2003), 41, <http://library.nps.navy.mil/uhtbin/hyperion-image/CCR202003.pdf>; <http://purl.access.gpo.gov/GPO/LPS31758> (accessed November 27, 2005).

²⁴ General Accounting Office, *Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies* (Washington, D.C: General Accounting Office, 2003), 1, <http://www.gao.gov/new.items/d03139.pdf> (accessed November 27, 2005).

²⁵ General Accounting Office, *Homeland Security: CDC's Oversight of the Select Agent Program* (Washington, D.C.: General Accounting Office, 2002), 1, <http://www.gao.gov/new.items/d03315r.pdf> (accessed November 27, 2005).

²⁶ Federal Bureau of Investigation, *Amerithrax*.

²⁷ See *Amerithrax* for a complete account of the FBI/EPA investigative protocols used during the search.

reveals shortfalls in national systems for disease detection. The 2001 U.S. anthrax attacks “tragically confirmed the importance of disease surveillance, since the speed with which doctors recognized the signs of anthrax infection determined whether patients were treated immediately or sent home, only to return later to die.”²⁸ It also stressed the significance of improving domestic defenses, especially since “many tools used to address natural disease threats will be needed to respond to an intentional attack.”²⁹

In closing remarks before a congressional subcommittee on November 6, 2001, RAND policy analyst John Parachini said the anthrax attacks represented “a fundamental shift in the nature of the biological terrorism threat.”³⁰ He concluded the attacks should prompt government action to strengthen nonproliferation, to deny and dissuade state and sub-national groups from using biological weapons, and to “develop rapid means to detect an attack and track down the perpetrator should preemptive and preventive measures fail.”³¹ This thesis focuses on the later, which is detection and attribution through improved surveillance and interagency cooperation.

B. METHODOLOGY AND SOURCES

This thesis proceeds in an inductive fashion. Preliminary comparison of the cases reveals a pattern of independent, dependent, and intervening variables. The Rajneesh attack was covert, while the anthrax letters were overt. The Rajneesh used a non-lethal Category B agent, whereas the Amerithrax attacks used a deadly Category A agent.³² The salmonella event was for the most part undetected and entirely unattributed to bioterrorism, while the anthrax episodes were more quickly detected and immediately attributed to a BW attack. Case comparison shows that *nature of attack* (overt vs. covert) and *agent type* (lethality) are independent variables that cause or facilitate the dependent variables of *detection* and *attribution*. Moreover, medical *surveillance* serves as an intervening variable for detection, whereas interagency *cooperation*, e.g., between the

²⁸ Christopher Chyba, “Toward Biological Security,” *Foreign Affairs* 81 (May/June 2002): 131.

²⁹ *Ibid.*, 122.

³⁰ John Parachini, *Anthrax Attacks, Biological Terrorism, and Preventive Responses* (Santa Monica, CA: RAND Corporation, 2001), 17, <http://www.rand.org/publications/CT/CT186/> (accessed October 15, 2006).

³¹ *Ibid.*

³² See <http://www.bt.cdc.gov/agent/agentlist-category.asp> for an explanation of CDC agent classifications.

public health system and law enforcement, serves as an intervening variable for attribution. The cases are run through each variable to illustrate a notional model of biodefense in Chapter IV. Inductive reasoning will show that medical surveillance, epidemiology, and the public health sector's coordination with emergency services and law enforcement are essential improvements to shore up U.S. biodefense strategy.

This thesis defines detection as the regional or national awareness of an outbreak. Most outbreaks are effectively detected and managed locally.³³ A challenge to U.S. biodefense is outbreaks involving cases over a wider area or in multiple local health jurisdictions. These may be easily missed, particularly if the isolated epidemics are characterized by a slowly rising number of cases.³⁴ This thesis also defines surveillance as a regional or national concern, as surveillance enables detection. Classical means of medical surveillance include sentinel labs and clinician reporting after disease diagnosis. Modern methods include “syndromic surveillance,” which covers a host of activities to monitor illness such as over-the-counter medication purchases that can forewarn of bioterrorism.³⁵ The goal is earlier detection and a timelier public health response, “hours or days before disease clusters are recognized clinically, or before specific diagnoses are made and reported to public health authorities.”³⁶ Authorities agree that increasing surveillance for human and animal pathogens is vital for addressing the menace of bioterrorism.³⁷ This is not only because of the demonstrated threat, but also because of emerging, reemerging, and antibiotic resistant disease. Population shifts, urbanization,

³³ Marc-Alain Widdowson et al., “Automated, Laboratory-Based System using the Internet for Disease Outbreak Detection, the Netherlands,” *Emerging Infectious Diseases* 9, no. 9 (September 2003), <http://www.cdc.gov/ncidod/EID/vol9no9/02-0450.htm> (accessed October 15, 2006).

³⁴ Ibid.

³⁵ As of May 2003, CDC estimates U.S. health departments have initiated syndromic surveillance systems at approximately 100 sites throughout the country. James W. Buehler et al., “Syndromic Surveillance and Bioterrorism-Related Epidemics,” *Emerging Infectious Diseases* 9, no. 10 (October 2003), <http://www.cdc.gov/ncidod/EID/vol9no10/03-0231.htm> (accessed October 15, 2006).

³⁶ Ibid.

³⁷ Jessica Stern, “Confronting Biological Terrorism: Global Epidemiological Monitoring,” *Harvard International Review* 23, no. 1 (2001), <http://hir.harvard.edu/articles/1008/> (accessed October 15, 2006).

poverty, and international travel and trade also facilitate the movement of microbes to new areas and hosts, “further complicating the task of identifying the source of infectious disease.”³⁸

Attribution is defined as a two-level process. The first tier is differentiating between a natural disease outbreak and a malicious attack. Outbreaks must first be detected and characterized as terrorism. While this seems obvious in theory, history and the case studies show it to be more difficult in practice. The second tier is actually tracing back to the perpetrator—the so called ‘return address’ capability. In sum, the Rajneeshee case never got past the first stage to even attempt the second, and underscores the need for effective communication and coordination between intelligence, public health, and law enforcement officials. The first level of attribution relies more heavily on organizational theory than science, is well within our national capabilities, and represents the first line of defense and focus of this thesis.

Recent U.S. laws, presidential directives, national strategy documents, government reports, congressional testimonies, agency briefings, and personal interviews were all used as sources of information. The evolution of applicable laws, directives, and strategy documents over the past ten years were also evaluated and applied. Observation and participation in public health exercises also contributed to the thesis. These include direct participation in California’s “Golden Guardian” emergency response exercise held in San Francisco on November 15, 2006, as well as bioterrorism-related table-top exercises held at the Monterey Institute of International Studies in February 2005.

C. THESIS ORGANIZATION

This thesis consists of five chapters. Chapter I defines the problem and explains its importance, establishes the methodology of argument, and introduces the work’s key findings. These are supported by case studies in Chapters II and III, and by literature review, exercise participation, and interview information which is presented in Chapter IV. Chapter V concludes by synthesizing the results. It provides policy recommendations intended to enable a comprehensive U.S. biodefense strategy.

³⁸ Stern, *Confronting Biological Terrorism*.

Chapter II examines the Rajneesh cult biological attacks. More than any other, this case demonstrates the inextricable link between an organization's objectives, its agent selection, and ultimate outcomes. It shows the failure of nonproliferation regimes, international and domestic security protocols, and national defense strategies to deter certain types of actors and prevent low-grade BW attacks. It also reveals that mass casualties are not always the objective. On the contrary, the Rajneeshees went to great lengths to remain stealth and produce no death. Finally, this chapter shows the importance of attribution—a tough lesson learned from poor interagency coordination during the criminal investigation which began a full year after the attacks.

Chapter III covers the U.S. anthrax attacks. It illustrates the costly long-term effects to government and society from a relatively simple one-off attack. Amerithrax shows that determined actors—whether state-sponsored, transnational, domestic, or lone-wolf—will not yield in the quest for biological weapons. They are aptly maneuvering through or around the four necessary capabilities. More than any other case, Amerithrax provides a glimpse into the future of countering bioterrorism. It marks the beginning of special investigative protocols between medical, public health, environmental, and law enforcement communities. It highlighted infrastructure shortfalls that prompted today's biodefense initiatives including Projects BioShield, BioWatch, and BioSense; refinements in the Strategic National Stockpile and Laboratory Response Network, and creation of the National Biological Analysis and Countermeasures Center.

Chapter IV explains a notional model of biodefense and examines the current U.S. strategy. The composition and limitations of the U.S. public health system are studied. These deficiencies are compared to 1) lessons learned from the case studies, and 2) current biodefense policy, infrastructure improvements, and programs to expose remaining shortfalls in preparedness. These areas combined reflect our nation's ability for *detection* of biological attacks. The chapter then turns to analysis of law enforcement's integration with public health. It uses the case studies to show the often diametrically opposed missions in these fields, and draws upon direct participation in bioterror emergency response exercises to demonstrate impediments to effective coordination. This, in turn, reflects our nation's ability for *attribution* of biological attacks.

Chapter V concludes by providing policy recommendations. These call for increased national laboratory capacity and incentives for rapid reporting and information sharing. A two-pronged approach is recommended that combines financial incentives with joint exercise and training. The emphasis here is on building trusted networks of intelligence, law enforcement, medical, and public health officials—networks that span the bridge separating policy and culture on one side, from evidence and science on the other.

II. THE RAJNEESHEE CULT BIOLOGICAL ATTACKS

Terrorists want a lot of people watching and a lot of people listening, but not a lot of people dead...[explaining why]...terrorists have not done some of the terribly damaging and terrifying things they could do, such as poisoning a city's water supply, spreading chemical or biological agents, or other things that could produce mass casualties.³⁹

A. INTRODUCTION

In September 1984, the Rajneeshees succeeded in conducting the first documented bioterror incident in the United States. The town of The Dalles, Oregon was bewildered by widespread food poisoning from salad bar contaminations that produced symptoms ranging from nausea and diarrhea to headache and fever. Until then, there had been only 222 bioterror-related incidents in the United States with only 24 being confirmed attacks. Of these, only the Rajneeshees' use of a crude biological weapon resulted in significant nonfatal casualties, causing 45 to be hospitalized and 751 to fall ill.⁴⁰ Even today, their attacks serve as a defining moment for bioterrorism in the United States.

This chapter begins by summarizing the case. The cult's organizational structure and key players, their motivations, and the group's intentions are reviewed. Nature of attack and target selection are considered next. The incident shows how covert strikes can leverage time and incubation periods to result in more casualties than overtly announced BW attacks. With regard to target selection, the cult's unimpeded success against a human population raises serious critical infrastructure protection questions about less protected U.S. livestock and crop formations. The group's agent selection decision and means to acquire and produce biological weapons are also studied. Finally, the surveillance/epidemiology and detection/attribution thesis elements are evaluated in light of the Rajneeshee case. The chapter conclusion discusses distinct findings that can be learned and applied to bolster U.S. biodefense strategy.

³⁹ Brian M. Jenkins, "International Terrorism: A New Mode of Conflict," in David Carlton and Carlo Schaerf, eds., *International Terrorism and World Security* (London: Croom Helm, 1975), 15, and Brian M. Jenkins, "Will Terrorists Go Nuclear?," *Orbis* 29, no. 3 (1985), 507-15.

⁴⁰ Parker, *Agricultural Bioterrorism*, 19.

B. CASE SUMMARY

1. Organization and Key Players

Chandra Mohan was born in Madhya Pradesh, India, in December 1931. In 1953 he took the name “Bhagwan Shree Rajneesh,” and later established the Acharya Rajneesh Ashram organization in 1974.⁴¹ The Indian spiritual leader based his teachings on the traditions of Buddha, Krishna, Jesus, Zen masters, Hassidism, and Sufism.⁴² The “Enlightened Master’s” spiritual regimen was based on meditation and uninhibited sexuality. His cult gained an international following and became increasingly notorious in Poona, India, the site of its first commune or “ashram.” By the 1980s, the Rajneeshees faced growing hostility and were being pursued by the Indian government for tax evasion.

The Bhagwan’s personal secretary and most trusted follower was Sheela P. Silverman, otherwise known as Ma Anand Sheela.⁴³ In 1981 Ma Sheela convinced the Bhagwan to immigrate to the United States in search of a new home for the cult. The group operated from a New Jersey mansion before deciding on a suitable location for the new ashram.⁴⁴ It was Sheela who decided to purchase a property in Oregon known to locals as the Big Muddy Ranch. Although the land straddled both Jefferson and Wasco Counties, the major portion was in Wasco, a largely rural area with a population of approximately 20,000. The county seat was a small town called The Dalles, which in 1985 had a population of about 10,000 and is located just over an hour’s drive east of Portland on Interstate 84. The plan was to build a “Buddhfield” or agricultural commune where the Rajneeshees could celebrate the enlightened master’s philosophy of “beauty, love, and guiltless sex.”⁴⁵

⁴¹ Zilinskas, *Biocriminality and Bioterrorism*, slides 25-29.

⁴² Answers.com, “Rajneesh,” <http://www.answers.com/topic/rajneesh> (accessed September 20, 2006).

⁴³ *The New York Times*, “Former Aides to Guru in Oregon Plead Guilty to Numerous Crimes,” http://topics.nytimes.com/top/reference/timestopics/subjects/i/immigration_and_refugees/index.html?query=ONANG,%20DIANNE%20Yandfield=perandmatch=exact (accessed September 20, 2006).

⁴⁴ W. Seth Carus, “The Rajneeshees (1984),” in *Toxic Terror: Assessing Terrorist use of Chemical and Biological Weapons*, ed. Jonathan B. Tucker (Cambridge, MA: MIT Press, 2000), 116-8.

⁴⁵ Judith Miller, Stephen Engelberg, and William Broad, *Germs: Biological Weapons and America's Secret War* (New York, NY: Simon and Schuster, 2001), 15.

In 1982 the Bhagwan began to operate under a self-imposed four-year vow of silence. Consequently, he was not directly involved in the day-to-day operations of the organization. Ma Sheela ran much of the commune in his name and her power came from meetings she held every evening with the cult leader. Sheela was the only person not in the Bhagwan's immediate household who had daily contact with him. It was widely understood among Rajneeshees that Sheela represented the Bhagwan, and he confirmed that she spoke in his name when doubts arose about her authority.⁴⁶ Despite her favor in the Bhagwan's eyes and sweeping powers throughout the community, two groups emerged in opposition. First was the Bhagwan's personal household including a handful of people and his personal physician Devaraj. Sheela resented this group because of its personal closeness to the cult leader. The second group, known as the "Hollywood Crowd," consisted of people whose wealth and fame provided special access to the Bhagwan. Ma Prem Hasya led this crowd and was married to a famous Hollywood producer. Eventually an alliance formed between the two opposition groups when Hasya married the household physician Devaraj.⁴⁷

Ma Sheela ruled large number of "moms" and more senior "big moms" for which she relied to direct daily operations of the commune.⁴⁸ Only one senior member was male besides the Bhagwan himself. David Berry Knapp, otherwise known as Krishna Diva or "K.D.," served as mayor of what would later become the municipality of "Rajneeshpuram." Of the big moms, Dianne Y. Onang, also known as Ma Anand Puja, was the darkest character in the group.⁴⁹ A licensed family nurse practitioner and registered nurse, Ma Puja joined the cult in India in 1979. Puja enjoyed a special social bond with Sheela despite being a recluse who took meals alone. She was an integral part of the inner circle running the community and held several important positions within the cult. As vice president of the Bhagwan's church, Rajneesh Foundation International, she was one of few members who had the power to appoint or remove trustees.⁵⁰ More

⁴⁶ Carus, *The Rajneeshees*, 119.

⁴⁷ Ibid., 120.

⁴⁸ Ibid., 119.

⁴⁹ *The New York Times*, *Former Aides to Guru in Oregon Plead Guilty to Numerous Crimes*.

⁵⁰ Carus, *The Rajneeshees*, 121.

importantly, Puja wielded absolute control over all medical facilities in the organization, including the Pythagoras Clinic and Pythagoras Pharmacy of the Rajneesh Medical Corporation. In 1980 she became director of the Shree Rajneesh Ashram Health Center and quickly became known as the cult's "Dr. Mengele."⁵¹ K.D. recalled that Puja 'delighted in death, poisons, and the idea of carrying out various plots.' Her fascination with the AIDS virus may have actually resulted in one human trial. In FBI interrogation transcripts, K.D. testified that Puja was always very excited about the disease. She questioned medical personnel about culturing the AIDS virus according to evidence obtained by law enforcement officials. Although she purchased a quick-freeze dryer in September 1984, it is unlikely she ever successfully cultured AIDS. Even so, "there are unconfirmed reports she may have deliberately infected at least one individual with the HIV virus to see if it was possible to transmit the disease."⁵²

The Rajneeshee organization and its working relationships between leader and senior managers are important. Table 1 below shows the key players and their alleged roles in the organization's biological weapons program.

Participants	Activity		
	Planning	Culturing Agent /	Spreading BW Agent
Anugiten	X	X	X
Ava	X	?	X
Bhagwan Shree Rajneesh	?		
Bodhi			X
Jayanda	?		
Julian	X		X
K.D.	X		X
Parambodhi		X	
Puja	X	X	X

⁵¹ Carus uses this as a reference to the notorious Nazi concentration camp doctor to show the depth of animosity that her Puja's behaviors generated among those in the commune. Carus, *The Rajneeshees*, 121.

⁵² Ibid., 126-7.

Participants	Activity		
	Planning	Culturing Agent /	Spreading BW Agent
Savita	X		
Sheela	X		X
Su	X		
Vidya	X		
Yogini	X		?

Table 1. “Alleged Participants in Salmonella Contamination Activities.” (From: W. Seth Carus, Table 8.1 in *The Rajneeshees* (1984), 125.)

An organization theory model of terrorist motivations says that bureaucracies contain self-interested and competing subunits.⁵³ Internal compartmentalization and competition place limits on the organization to coordinate action and make rational decisions. Over time, organizations may lose sight of strategic objectives—confusing ends with means and pursuing violence merely for violence’s sake—as leaders lose both doctrinal and tactical control. The Rajneeshee case perfectly illustrates all of these points. In sum, a cluster of only 14 persons executed a plan of three key players in an organization numbering 4,000 members. The Bhagwan’s vow of silence and hands-off approach gave Ma Sheela power to push her agendas. Ma Puja’s dark side, her technical expertise, and special connection with Sheela enabled her to coax the group towards bioterrorism. Finally, K.D.’s public relationship with outsiders as mayor of Rajneeshpuram motivated him to constrain the others. Although he actively participated in the attacks, it was K.D. who convinced Sheela and Puja to avoid deadly pathogens for fear the cult would be immediately suspected. An examination of the group’s motivations and intentions are necessary to better understand their organizational structure, the key players, and their influence on the type of attack and agent to be used.

2. Motivations

The Rajneeshees had substantial financial resources. The Bhagwan was known as “the rich man’s guru,” because many of his followers were affluent and turned over all their assets to the cult. The group also earned considerable income from the sale of

⁵³ Stern, *Terrorist Motivations and Unconventional Weapons*, 202-29.

books and tapes on the Bhagwan's teachings. The most devoted followers were "sannyasins," who dressed only in shades of red and worked 12-hour days chanting songs and proclaiming loyalty to the Bhagwan.⁵⁴ It was on the backs of the sannyasins that the Rajneesh built what amounted to a small city. Their communal system was supported by vast infrastructure including a dam and lake, networks of roads, sophisticated water, sewage, and transportation systems; and an airstrip on the valley floor for the cult's five jet planes and helicopter.⁵⁵ The ranch's 350-million gallon reservoir fed 14 irrigation systems. This supported farms which provided 90 percent of the community's food. The cult also operated a ten-megawatt power station and fielded a fleet of 85 buses for its transportation needs.⁵⁶ Finally, community amenities included a 2.2-acre meeting hall, a 160-room hotel, a two-block-long shopping mall, and a casino and disco.⁵⁷

The Rajneeshees used the legal system to meet their needs when friendly tactics and diplomacy failed. They were extremely litigious, suing for the smallest provocation and flooding courts with cases to steamroll and intimidate opponents.⁵⁸ Rajneesh Investment Corporation teamed with Rajneesh Foundation International to spearhead and coordinate legal attacks. Deputy county clerk Karen LeBreton estimated that 60 percent of her work included responding to Rajneeshee legal suits and petitions.⁵⁹ On the other hand, the group disregarded laws that interfered with its objectives. Sham marriages to conceal members brought the cult squarely into conflict with the U.S. Immigration and Naturalization Service and U.S. Attorney's Office in Portland, Oregon. In addition, the group registered as a religion to leverage tax benefits despite years of condemning organized religion.⁶⁰

In spite of their strange beliefs and often disturbing public displays of sexual freedom, some locals tolerated the Rajneeshees because they brought doctors, lawyers,

⁵⁴ Miller, Engelberg and Broad, *Germes*, 16.

⁵⁵ Ibid.

⁵⁶ Zilinskas, *Biocriminality and Bioterrorism*.

⁵⁷ Miller, Engelberg and Broad, *Germes*, 16.

⁵⁸ Carus, *The Rajneeshees*, 118.

⁵⁹ Miller, Engelberg and Broad, *Germes*, 22.

⁶⁰ Carus, *The Rajneeshees*, 118.

and engineers to the area.⁶¹ Also, their massive spending amounted to a local investment of more than \$35 million in construction efforts at the ranch since the cult's arrival. This was a tremendous financial boost to The Dalles since its sole industry, an aluminum smelting plant, had shut down two years prior. There was only one problem with the cult's impressive expansion. It flew in the face of rural zoning ordinances which applied to their property. The cult built anyway, despite failing to win the favor of Wasco County commissioners and securing the necessary permits. The Rajneeshees soon found themselves in a protracted series of political and legal disputes, many of their own making. They had a rational plan to solve all of their problems by fighting politics with politics.

To evade zoning restrictions, the Rajneeshees took over the nearby town of Antelope in 1982 along with its school district.⁶² It was easy to move enough people into the small community of 75 and outnumber the existing inhabitants by exploiting Oregon's liberal voter-registration laws. The cult instituted several measures that angered residents after securing electoral control of the town. These included renaming Antelope and its school district "Rajneesh," and insisting that council meetings begin and end with a joke.⁶³ They also turned Antelope's sole business into a vegetarian health-food café called Zorba the Buddha. Infuriated citizens responded with bumper stickers saying "BETTER DEAD THAN RED" and "MONEY CAN'T BUY ANTELOPE'S HERITAGE."⁶⁴ The second stage of their plan was to incorporate the commune at Big Muddy ranch into a township called "Rajneeshpuram." The new jurisdiction and legal status of the municipality conveyed significant benefits. Now the cult was able to field not one, but two authorized police forces—one at Rajneesh (Antelope) and one within the commune at Rajneeshpuram. More alarming was the legal access this afforded them to state law enforcement and medical assets.

A select 150 members of the cult began carrying arms to address concerns that the FBI might try to kidnap the Bhagwan. In addition, Rajneeshpuram's 60-member "Peace

⁶¹ Miller, Engelberg and Broad, *Germs*, 17.

⁶² Carus, *The Rajneeshees*, 118.

⁶³ Miller, Engelberg and Broad, *Germs*, 16.

⁶⁴ *Ibid.*

Force” was well equipped with military hardware such as Uzi’s and Kalashnikov machine guns.⁶⁵ Oregonians who drove county public roads adjacent to cult property complained of being stopped and harassed by the Bhagwan’s police. His Peace Force and other legally armed officers enjoyed access to state-run law enforcement training programs and Oregon’s crime data networks. Fortunately, the FBI denied access to sensitive information on its National Crime Information Center database due to ongoing federal investigations into civil-rights complaints against the cult.⁶⁶ Rajneeshpuram ultimately became the center of legal disputes between the cult and Oregon’s Attorney General David Frohnmeyer, who concluded there was no separation between church and state in their jurisdiction. The community was therefore unconstitutional. For the Rajneeshees, diplomacy had failed and political maneuvering had reached an impasse. With time running short and desperation setting in, the cult quickly escalated to violence to preserve their community’s sense of autonomy, control, and power. These motivations breed intentions that were aimed at taking political control of the county seat and government.

3. Intentions

Ma Sheela and the Bhagwan decided to take control of the Wasco County Commission by winning the upcoming November 1984 elections. By some means, 4,000 members of the commune (many of whom were not U.S. citizens and could not vote) needed to take over a county of 20,000 inhabitants including some 15,000 registered voters.⁶⁷ K.D. insisted on voter fraud and three schemes were considered. First was a plan to rent apartments throughout Wasco County and register Rajneeshees under multiple names to vote several times during the elections. Elements of this plan included using disguises and absentee ballots to avoid detection. The risk was considered too great and this plan was rejected. The second proposal involved running a candidate for County Commissioner that would support Rajneeshee interests. This failed when the group was unable to secure the required number of signatures to get their candidate on

⁶⁵ Miller, Engelberg and Broad, *Germs*, 31.

⁶⁶ Ibid., 17.

⁶⁷ Carus, *The Rajneeshees*, 122-3.

the ballot. Along these lines, the cult also considered having one of its members, Ma Jagruti, run for office under an assumed name. This was also abandoned when Oregon officials learned that Jagruti voted fraudulently in a previous election.⁶⁸

Ma Sheela, influenced by Ma Puja, came up with the third idea of making citizens sick before the elections so they would be unable to vote. K.D. told investigators that Sheela talked with the Bhagwan about a plot to decrease voter turnout by making people sick.⁶⁹ She played tape recordings to the disciples of her meetings with the cult leader when doubts arose that he would support such a plot. When Sheela asked him what should be done to people who opposed the enlightened master's vision, he responded, "If it was necessary to do things to preserve [the Bhagwan's] vision, then do it... ." ⁷⁰ She also echoed his comments that it was best not to hurt people, but if a few died not to worry.⁷¹

Finally, a little known and seldom discussed aspect of the poisoning plan was the cult's "Share-A-Home" program. To augment the BW attack, the Rajneeshees would use their vast resources to import and house thousands of homeless. They would again exploit Oregon's weak voter registration laws by registering and harnessing the votes of these people. County officials outmaneuvered the group, however. Noting the submission of a large number of voter cards shortly before the registration period closed, officials insisted that all prospective new voters be questioned by a special panel at the town armory.⁷² The Rajneeshees were forced to abandon the scheme, realizing the homeless would not pass the test. What is more, with an awareness that their town was in trouble, Wasco County residents registered in record numbers. County turnout for the November 1984 election was proportionally the largest in Oregon history.⁷³

⁶⁸ Carus, *The Rajneeshees*, 123.

⁶⁹ Ibid.

⁷⁰ Quoted in Miller, Engelberg and Broad, *Germs*, 30.

⁷¹ Carus, *The Rajneeshees*, 123.

⁷² Miller, Engelberg and Broad, *Germs*, 31.

⁷³ Ibid.

C. NATURE OF ATTACK AND TARGET

Seldom discussed is that the attacks known as the “salad bar contaminations” or “restaurant attacks” were but one of several efforts by the Rajneeshees to gain political control. A series of gradual steps are taken when non-state actors endeavor to use biological weapons as shown in Figure 1.

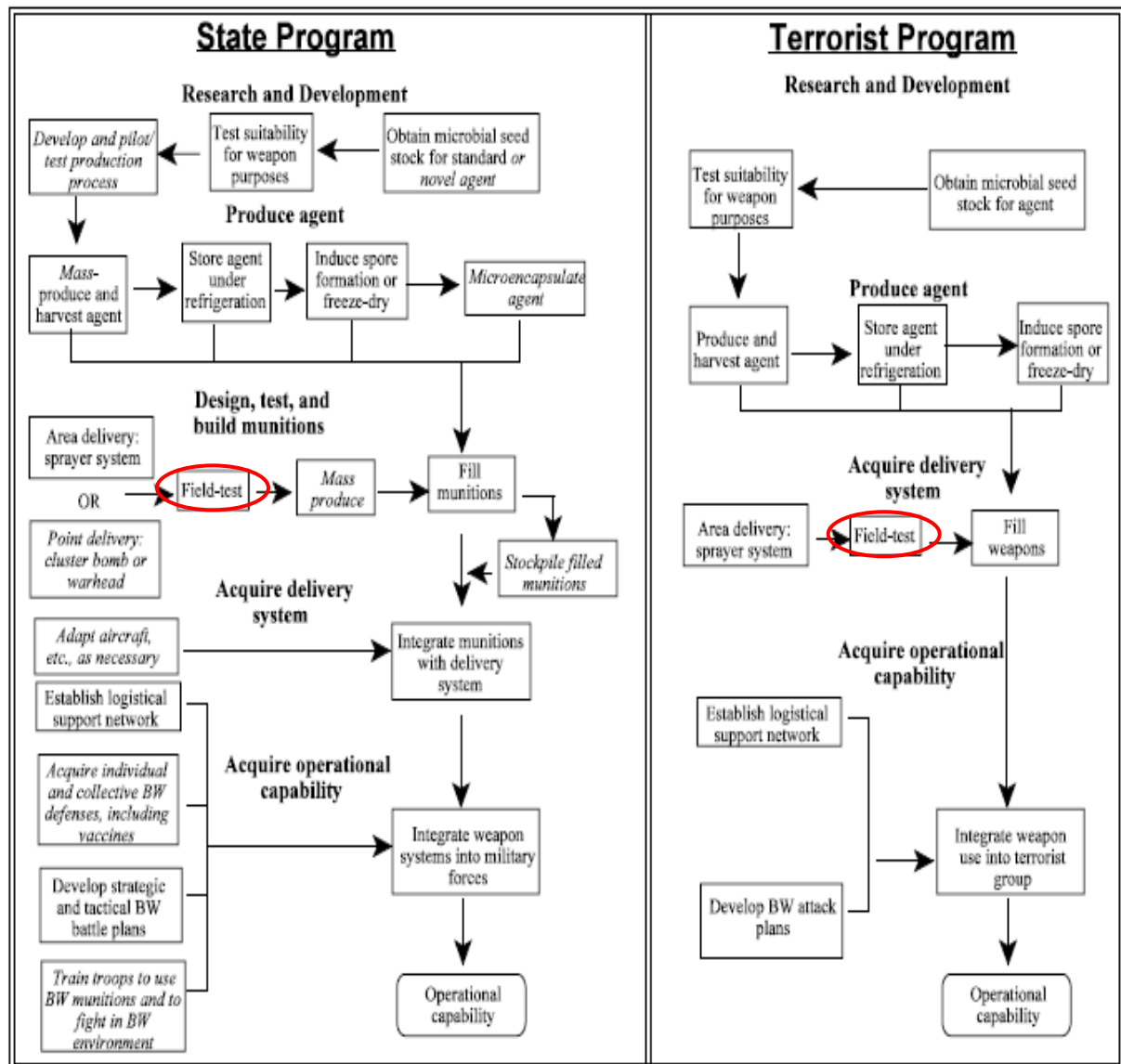


Figure 1. “Comparison of State Biological WMD and Terrorist Biological Agent Development.” (From: Congressional Research Service Report, *Small-scale Terrorist Attacks Using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons*, May 20, 2004, CRS-15.)

Acquiring and culturing agent stock seed, laboratory testing on animals, initial field testing on the target (whether human, livestock, or crop), larger public trial tests, and final operational attacks all represent typical patterns of a developing BW program. The restaurant contaminations were themselves public trials and only a precursor to the final planned operational attack on the town's water supply.

The first documented use of biological agents by the Rajneeshees occurred on August 29, 1984, during a routine fact-finding visit to Rajneeshpuram by three Wasco County commissioners.⁷⁴ The cult gave water laced with salmonella to Judge William Hulse and Raymond Matthews, the two commissioners most unfavorable to the group. Both became sick and Judge Hulse required hospitalization. The restaurant attacks occurred in two distinct waves in the following month. The Dalles' location along Interstate 84, a major east-west transportation route 90 miles east of Portland, Oregon, produced an environment with more restaurants than normal for a town of its size with 35 establishments in all.⁷⁵ Ten restaurants were contaminated with salmonella during the cult's trial runs.

K.D. and accomplice Ma Ava described their direct participation in the attacks to FBI and Oregon state investigators, along with the involvement of Ma Sheela and Ma Puja. By his own admission, K.D. participated after Puja gave him "a plastic bag containing a test tube sealed with a cork stopper and filled with a 'mostly clear' light brown liquid."⁷⁶ Puja ordered him to spread the vial at restaurants in town. "During a trip into town to attend a meeting with another cult member, K.D. went to the Portage Inn. Because they arrived after lunchtime, the salad bar was closed, but he poured the contents of the vial into the salad dressing."⁷⁷ K.D. told officials that Puja wore a wig and tainted the salad bar at the Recreation Café. For her part, Ava contaminated three restaurants at Sheela and Puja's request. She and cult member Swami Satyam Bodhidharma drove to The Dalles with five or six vials of "salsa."⁷⁸ According to Ava's

⁷⁴ Carus, *The Rajneeshees*, 128.

⁷⁵ Miller, Engelberg and Broad, *Germs*, 19.

⁷⁶ Quoted in Carus, *The Rajneeshees*, 129-30.

⁷⁷ Ibid.

⁷⁸ Ibid.

sworn testimony, they poured their vials into coffee creamers at Johnny's Café and The Chuck Wagon restaurants. They also contaminated blue cheese salad bar dressing at Arlo's restaurant. Ava said Puja claimed to have put salmonella in "lots of places," and on at least one mission a cult member saw Puja change into a disguise.⁷⁹ Others were also involved in the restaurant attacks.⁸⁰

The main objective was a critical infrastructure attack on the town's water supply. Sheela ordered K.D. to acquire maps of The Dalles' water system. Ava recalls seeing a lot of empty cages in the medical center's laboratory along with Puja contacting the Rajneeshpuram Resource Manager to obtain raw sewage. Moreover, two other cult members named Julian and Anugiten conducted two trials to contaminate the town's water supply.

According to K.D., Julian described how he and Anugiten climbed up a hill to a water tank that overlooked a nearby school. He recalled something being mentioned about trying to pry open the screen on the water tank and hearing rushing water. ...[Ava] was ordered by Savita to pick up a car being held at the Portland Airport, clean it inside and out to eliminate any fingerprints, and park it at a specified parking spot in downtown Portland. Ava later concluded that this car had been used by Julian and Anugiten for one of their water-contamination operations.⁸¹

At some point in late September or early October 1984, the Rajneeshees' biological aspirations began to wane and the cult shifted to more conventional tactics. Interestingly, the administrative and logistical demands of the "Share-A-Home" program played a key role in the group's decision to abandon the use of biological agents.⁸² After the restaurant contaminations the cult targeted individuals, such as Portland U.S. Attorney Charles H. Turner. Turner was on Sheela's short list of rivals to be eliminated, and the Rajneeshees actually acted on their plans to silence him. Members traveled to Texas to purchase handguns but found it difficult to purchase with out-of-state

⁷⁹ Quoted in Carus, *The Rajneeshees*, 129-30.

⁸⁰ Ibid.

⁸¹ Ibid., 133.

⁸² Ibid., 137.

identification. They continued to New Mexico, obtained false identification, and bought several pistols. The plan was to assassinate Turner in the garage of a federal building but the plot was foiled by law enforcement officials.⁸³

D. AGENT SELECTION AND ACQUISITION

Ma Puja considered several agents including ones to cause typhoid fever (*Salmonella typhi*), hepatitis, and even AIDS.⁸⁴ K.D. insisted on ruling out typhoid and hepatitis for fears of them being traced back to the cult. AIDS was discarded by Puja because of its difficulty to culture and weaponize. Puja's team also considered putting dead rodents into The Dalles' water supply. Beavers were preferred because they naturally carried bacteria in their bodies called *Giardia lamblia* or "beaver fever," but they were too big to fit through screens on the town's water tanks.⁸⁵ Infected rats and mice were also considered. The agent finally selected was *Salmonella enterica* serotype typhimurium—a bacteria strain common in food poisoning.⁸⁶ Rajneesh Medical Corporation (RMC) lab technician Parambodhi provided technical expertise and assisted Puja in culturing the salmonella.⁸⁷ He initially objected saying it was too dangerous, but later reluctantly agreed to grow it for Puja.

The RMC purchased a set of "bactrol disks" from VWR Scientific, a medical supply company in Seattle, Washington.⁸⁸ The salmonella known as American Type Culture Collection (ATCC) number 14028 was commonly used in medical settings. Puja and Parambodhi used the disks in the RMC's state-licensed medical laboratory to culture and mass-produce the final weapon. The RMC had a legal and supposedly legitimate need for the substance, because it was a control organism used to meet the requirements for quality assurance expected of licensed clinical labs. Puja and the RMC were required by law to test the proficiency of their technicians by having them identify samples

⁸³ Quoted in Carus, *The Rajneeshees*, 136.

⁸⁴ Ibid., 124-7.

⁸⁵ Cult members actually joked about chopping up and mixing the beavers in blenders to solve this problem. Ibid., 126.

⁸⁶ Ibid., 124.

⁸⁷ Ibid., 128.

⁸⁸ Ibid., 127.

contaminated with known agents. Licensed labs maintain stocks of common pathogens for just this purpose. They also use such organisms to ensure the quality of growth media used in their diagnostic testing.

Because of her position and the RMC's status, Puja could buy certain classifications of agents without suspicion from companies such as VWR Scientific. She even obtained dangerous pathogens from the ATCC, which at the time was a "giant private germ bank located first in Maryland and later in Virginia from which doctors, clinics, and hospitals order germs for research and standard diagnostic tests."⁸⁹ An invoice from the ATCC showed the cult ordered and received a variety of pathogens, some even deadly such as typhoid fever. Puja also secured orders for *Enterobacter cloacae* (responsible for various infections including bacteremia, lower respiratory tract infections, skin and soft tissue infections, and urinary tract infections),⁹⁰ *Neisseria gonorrhoeae* (gonorrhea), and *Shigella dysenteriae* (shigellosis).⁹¹

Large-scale production took place in the "Chinese Laundry" of Rajneeshpuram, and was later moved to the Alan Watts complex which consisted of approximately two dozen buildings in the northeast section of the commune.⁹² The actual facility for producing the salmonella consisted of two A-frame structures connected by a common bathroom. Ava described a large freeze dryer and "a green incubator the size of a small apartment-type refrigerator" containing petri dishes used to grow the bacteria.⁹³ She also recalls receiving two large jars filled with liquid containing salmonella salsa. Cult officials identified the site as a germ warfare laboratory during the subsequent criminal investigation.⁹⁴

⁸⁹ Miller, Engelberg and Broad, *Germs*, 26.

⁹⁰ Susan L Fraser, "Enterobacter Infections," EMedicine, August 6, 2006, <http://www.emedicine.com/MED/topic678.htm> (accessed November 27, 2006).

⁹¹ "Fewer than one hundred organisms of shigella are needed to cause very severe dysentery – profuse diarrhea, bloody mucoid stools, and cramping – and death in as many as 10 to 20 percent of cases, even in previously healthy persons." Miller, Engelberg and Broad, *Germs*, 27.

⁹² Carus, *The Rajneeshees*, 127-8.

⁹³ Quoted in Carus, *The Rajneeshees*, 128.

⁹⁴ Ibid.

E. SURVEILLANCE AND EPIDEMIOLOGY

1. Initial Reports

On September 17, 1984, the Wasco-Sherman Public Health Department received its first call from someone complaining of gastroenteritis after eating at a restaurant in The Dalles.⁹⁵ Twenty more illnesses from two more eating establishments followed within days. A pathologist at Mid-Columbia Medical Center identified salmonella from a patient's stool sample less than 48 hours after the outbreak began. Four days later, state public health scientists in Portland analyzed more samples and confirmed the presence of *Salmonella typhimurium*—a very unusual strain in this particular case nevertheless treatable with antibiotics. This was considered “speedy scientific sleuthing” since there are nearly 2,500 known strains.⁹⁶ Yet the outbreak would not be attributed to terrorism for another year, and then only due to public statements issued by Bhagwan Shree Rajneesh.

Carla Chamberlain, the nurse who ran the county public health office, knew that between 1980 and 1983 her department reported only 16 isolates of salmonella. Of these, only eight were *Salmonella typhimurium* and none resembled this particular strain.⁹⁷ County public health officials thought the outbreak was over when the epidemiological wave began to crest. However, the same day state lab technicians identified the exact strain in Portland, the county's public health department received a second wave of reports citing ten more restaurants in The Dalles.⁹⁸ The targeted establishments are shown in Table 2 on the following page.

⁹⁵ Miller, Engelberg and Broad, *Germes*, 18.

⁹⁶ Ibid.

⁹⁷ Ibid., 18-19.

⁹⁸ Ibid., 19.

Restaurants	
First Wave (September 11-18, 1984)	Arlo's Restaurant
	Portage Inn
Second Wave (September 19-25, 1984)	Arctic Circle Restaurant
	Arlo's Restaurant
	Burgerville USA
	Kopper Kitchen
	Pietro's Pizza Restaurant
	Portage Inn
	Recreation Café
	Shakey's Pizza Parlor
	Skipper's Seafood Restaurant
	Taco Time

Table 2. "Restaurant Contaminations Resulting in Illness in The Dalles, Oregon." (From: W. Seth Carus, Table 8.2 in *The Rajneeshees* (1984), 132.)

On September 25, 1984, in the midst of the second wave, the state sought help from the CDC and its Epidemic Intelligence Service (EIS).⁹⁹

2. First Response

Mid-Columbia Medical Center's lab was immediately overwhelmed and "stacked high with specimens destined for the state's laboratory in Portland... ." ¹⁰⁰ During the second outbreak the hospital went through three shipments of specimen media a week, instead of its normal one shipment every two or three weeks. "The twenty petri dishes of tests in a normal week mushroomed to two hundred every other day. At the peak of reports, the laboratory ran out of media altogether."¹⁰¹ Mid-Columbia's 125 hospital beds were filled for the first time ever, with some being kept in the corridors. Doctors struggled to treat panicked and even hostile patients. "Violent patients and their families

⁹⁹ In 1951 following the start of the Korean War, EIS was created as a warning system against biological warfare and man-made epidemics. It is composed of medical doctors, researchers, and scientists who serve 2-year assignments. Today the EIS mission includes surveillance and response for all types of epidemics including chronic disease and injuries. Centers for Disease Control and Prevention, "Epidemic Intelligence Service—About EIS," <http://www.cdc.gov/eis/about/about.htm> (accessed September 20, 2006).

¹⁰⁰ Miller, Engelberg and Broad, *Germs*, 19.

¹⁰¹ Ibid.

demanded their test results; some even threw stool and urine samples at the hospital's doctors and technicians.”¹⁰² This disturbing scene which occurred some 22 years ago vividly demonstrates the impact BW attacks can have on first responders and the medical system. Had symptoms been more severe or had the agent used been lethal, public hysteria and false reporting would have been exponentially worse. It should also be noted that today Mid-Columbia's capacity has been reduced from 125 hospital beds to 49.¹⁰³

3. Epidemiological Investigation

A substantial epidemiological investigation was conducted by EIS and the Wasco-Sherman County Public Health Department. The team questioned hundreds of patients, family members, and friends. Investigators also interviewed all 325 food handlers who worked at the ten restaurants, approximately 100 of which had been infected, and many of these falling ill before their patrons.¹⁰⁴ They located out-of-state visitors who purchased meals with credit cards to ascertain their condition and see what they consumed. Interviews were conducted with 120 people who ordered home delivery, as well as those who were served by the restaurants at banquets. None of these people were infected—it was only those who had eaten from salad bars.¹⁰⁵

Two local water systems and the water at restaurants were tested, and salad bar temperatures and food-handling practices were scrutinized.¹⁰⁶ Investigators visited farms that supplied cucumbers, tomatoes, and melons to the restaurants. They also checked a dairy in neighboring Washington State to test cows, cow feces, raw milk, and farm pond water. None of these contained the bacteria. A common source eluded investigators even though every item was traced back to its origin. The lettuce and other vegetables came from different suppliers, and the salad dressings were from different wholesalers. The team did find salmonella in the milk of coffee creamers in one café and in the blue

¹⁰² Miller, Engelberg and Broad, *Germes*, 19.

¹⁰³ *Ibid.*, 319.

¹⁰⁴ *Ibid.*, 20-21.

¹⁰⁵ *Ibid.*

¹⁰⁶ *Ibid.*

cheese dressing of another, but not in the dry mix used to make the dressing. “This suggested that the dressing had been contaminated during or after its preparation.”¹⁰⁷

4. Suspicions and Initial Epidemiological Reports

Both Carla Chamberlain and Judge Hulse were suspicious of the cult and its possible role in the outbreaks. According to hospital records, Judge Hulse was admitted and almost died a year earlier after his commission’s fact-finding visit to Rajneeshpuram. In a clandestine mission, Ava slipped salmonella into the judge’s breakfast at Zorba the Buddha café in Antelope the morning of his visit to the ranch.¹⁰⁸ The cult also gave him a tainted glass of water later that day at the ranch while they changed a flat tire on his vehicle in the hot sun. The tire, of course, was surreptitiously flattened by the cult during his visit. Chamberlain’s suspicions resulted from her visit with Puja at the RMC to discuss the county’s health reporting requirements and ensure their lab would comply. She was astonished to find that Rajneesh facilities were better equipped than that of the county.¹⁰⁹

Initial state public health investigator and CDC reports in the fall of 1984 and early 1985 concluded the Rajneeshees were not to blame for the outbreaks.¹¹⁰ Laurence Foster, the most senior state epidemiologist and widely respected figure in the regional medical community, was a staunch civil libertarian who “ardently believed that the Rajneeshees were being unfairly harassed because of their strange religious beliefs.”¹¹¹ Additionally, Foster was also the mentor of Thomas Török—one of the principal EIS team members dispatched to The Dalles leading the federal response. Foster’s preliminary report in November 1984 found no evidence supporting intentional contamination and concluded it was more likely that food handlers were responsible. While Foster did acknowledge finding no common source for infection, he deduced the cause “could have occurred where food handlers failed to wash their hands adequately

¹⁰⁷ Miller, Engelberg and Broad, *Germes*, 20-21.

¹⁰⁸ *Ibid.*, 29.

¹⁰⁹ *Ibid.*, 22.

¹¹⁰ *Ibid.*, 23.

¹¹¹ *Ibid.*, 22.

after bowel movements and then touched raw foods.”¹¹² Török’s EIS team concurred with these findings in their preliminary report issued January 1985, saying there was “no epidemiological evidence” supporting intentional contamination.¹¹³

F. DETECTION AND ATTRIBUTION

A full year later on September 16, 1985, the Bhagwan went public at the completion of his four-year vow of silence. In a press conference held at the ranch just two days after Ma Sheela and her allies resigned their posts and flew to Europe, he accused the lot of creating a “fascist regime” that plotted to kill fellow sannyasins, stole money, mismanaged commune affairs, and had left the cult some \$55 million in debt.¹¹⁴ More importantly, he publicly accused Sheela of poisoning his personal doctor and dentist, the district attorney of neighboring Jefferson County, and of trying to contaminate The Dalles’ water system. The Oregon Attorney General established a joint task force between state police and the FBI, obtained search warrants and subpoenas, and found the bactrol discs and laboratory equipment at the commune on October 2, 1985.¹¹⁵ Interestingly, it was about this time when the CDC filed its final report confirming that a single strain caused all of the illnesses in The Dalles.¹¹⁶ The potentially deadly pathogens such as *Salmonella typhi* (typhoid fever), *Enterobacter cloacae*, *Neisseria gonorrhoeae*, and *Shigella dysenteriae* were never found. The criminal investigation began a year following the attacks, leaving ample time for the Rajneeshees to destroy evidence. However, when the ATCC invoices were eventually seized in the search, they were not shared with public health officials who would have immediately recognized their significance in light of the criminal investigation. Public health officials learning of the invoices years later considered both the pathogens and timing of their arrivals at the RMC laboratory “ominous.”¹¹⁷

¹¹² Quoted in Miller, Engelberg and Broad, *Germes*, 25.

¹¹³ *Ibid.*, 23.

¹¹⁴ *Ibid.*

¹¹⁵ Thomas J. Török et al., “A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars,” in *Biological Weapons: Limiting the Threat*, ed. Joshua Lederberg (Cambridge, MA: MIT Press, 1999), 171.

¹¹⁶ Anderson, *The Rajneeshee Cult*.

¹¹⁷ Miller, Engelberg and Broad, *Germes*, 27.

Bhagwan Shree Rajneesh fled on October 27, 1985, and was arrested when his jet landed in Charlotte, North Carolina.¹¹⁸ With him were a few disciples and 21 suitcases containing a revolver, \$58,522 in multiple currencies, 35 jeweled wristwatches, and seven pairs of designer eyeglasses. Followers had also loaded his throne in the airplane. West German police detained Sheela and Puja at a luxurious resort hotel and extradition proceedings began. In the end, only Sheela and Puja were tried in criminal proceedings divided between state and federal courts. The Oregon Attorney General's Office took the poisoning cases of Judge William Hulse and Commissioner Raymond Matthews, while the U.S. Attorney's Office took the restaurant cases.¹¹⁹ On July 22, 1985, both Sheela and Puja pled guilty in state court to first-degree assault and conspiracy-assault for the poisoning of Judge Hulse. They also pled guilty to second-degree assault charges for the poisoning of Commissioner Matthews. "In total, Sheela received three concurrent twenty-year sentences, was fined \$400,000, and was ordered to pay Wasco County restitution in the amount of \$69,353.31."¹²⁰ For her part, Puja was sentenced to serve two concurrent 20-year sentences and a concurrent seven-and-a-half year sentence. The state pushed for time to be served in federal penitentiaries and also pursued separate civil proceedings against the cult. Shrewd bargaining by the defense resulted in the women serving less than four years in a jail for nonviolent white-collar offenders at Pleasanton, California Federal Prison. Sheela and Puja were released early on good behavior and fled once again to Europe before the Justice Department notified the state. The Bhagwan received a ten-year suspended sentence, was fined and paid \$400,000, and left the United States forever.¹²¹

Besides the reporting bias mentioned earlier, it is difficult to understand why this incident was not attributed to an intentional biological attack. Tensions between the cult and local community, combined with the concerns of county public health official Carla Chamberlain and Commissioner Judge William Hulse, should have sufficiently heightened suspicion. Between 1979 and 1980 the national survey included 233 strains

¹¹⁸ Miller, Engelberg and Broad, *Germes*, 31.

¹¹⁹ Carus, *The Rajneeshees*, 136.

¹²⁰ Ibid.

¹²¹ Miller, Engelberg and Broad, *Germes*, 32.

of *Salmonella typhimurium* with no antibiograms similar to the outbreak strain in The Dalles.¹²² This should also have been a warning. The double-crest of the epidemiological wave illustrated in Figure 2 should have been another anomaly suggesting foul play.

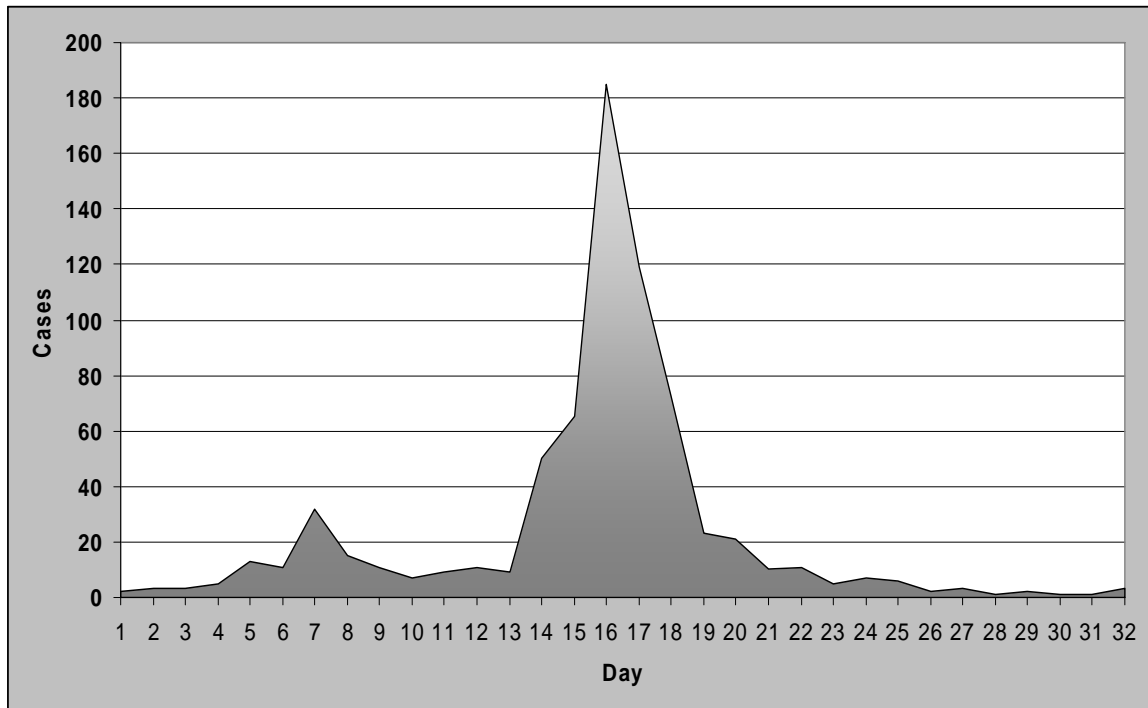


Figure 2. Rajneeshee Attack Epidemiological Curve. (From: Török et al., Figure 10.1 in *A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars*, 173.)

Note: Days six through eight correspond to September 14-16, 1984. Days 13-21 correspond to September 21-29, 1984.

Despite this a 1997 *Journal of the American Medical Association* article,¹²³ whose authors include original investigators Laurence Foster and Thomas Török, lists nine reasons the intentional contamination hypothesis was rejected:

- No apparent motive. Despite concerns of potential election fraud, the outbreaks in September and October were not obviously related to the November elections.

¹²² Török et al., *A Large Community Outbreak of Salmonellosis*, 178.

¹²³ The case study was originally a 1997 *Journal of the American Medical Association* article, then was later revised into a book chapter in 1999. *Ibid.*, 167.

- No one claimed responsibility and no demands were issued. If terrorism or extortion was a motive, public statements would have been issued to create widespread fear.
- Law enforcement investigators found few questionable activities reported from restaurant patrons and could not establish a recognizable pattern of unusual behavior.
- No disgruntled employees were identified, and the criminal investigation confirmed that employees did not intentionally contaminate food.
- Epidemic exposure curves indicated that salad bars were infected multiple times during a several-week period, suggesting a sustained source was necessary [although an opposite hypothesis could also be concluded].
- Some employees had onset of illness before patron exposures.
- To public health, EIS, and law enforcement knowledge, such an event had never happened. “We are aware of only two reports of foodborne illness caused by intentional contamination of biological agents, and neither incident appeared to be politically motivated.”
- The alternate hypothesis of intentional contamination, although less complicated, appeared less likely based on previously documented outbreaks.
- “Finally, even in thoroughly investigated outbreaks, the source sometimes remains occult, and, of all the reasons considered for failing to identify the source, this would be the most common.”¹²⁴

The benefits of hindsight, especially in today’s post-9/11 environment, make these findings appear unsound. However, the important questions to be asked are: 1) can another outbreak like the Rajneesh salad bar contaminations be prevented, and 2) if not, what is the best approach to deal with the possibility of covert attacks using unrestricted and readily available non-lethal agents? It is doubtful that regulation and control of commercially available pathogens would have prevented this or similar future attacks. Cultures such as the one used in The Dalles are easily obtained from clinical isolates or raw foods of animal origin in grocery stores.¹²⁵ Producing and storing large quantities of simple bacteria is inexpensive and requires basic equipment and technical skill. Finally, distribution and food handling practices of open societies are inadequate to prevent deliberate contamination by determined actors. This security-freedom tradeoff invites a

¹²⁴ Török et al., *A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars*, 183.

¹²⁵ Ibid., 184.

certain level of unmanageable risk. Bearing these in mind, the public is best served when health care professionals and laboratories communicate and cooperate with local and state health departments “to report notifiable disease and unusual disease clusters.”¹²⁶

The conclusion of Foster and Török’s report reveals an important finding from the Rajneeshee case that has implications for BW attribution.

Routine reporting is essential in disease surveillance at both the local and national level, and efforts to improve surveillance will assist in detecting future outbreaks in general. The epidemiological approach...need not be changed. The methods of determining pathogen, vehicle, and route of contamination and relating them to time, place, and person remain the same. On the basis of our experience in The Dalles, ...if investigation of a large cryptic outbreak implicates a mechanism of contamination that does not resemble established patterns, then the possibility of intentional contamination should be considered, and law enforcement agencies should be asked to consider undertaking an independent investigation.¹²⁷

The point is that customary “shoe-leather” epidemiological practices are proven and do not require change. However, when these investigative practices do uncover an anomaly, then a criminal act should be considered (attribution) and law enforcement should be advised.

G. CASE FINDINGS

Four distinct findings can be learned. First, the Rajneeshee attacks demonstrate more than any other case the inextricable link between organizational objectives, agent selection, and ultimate outcomes. The cult took a deliberate and *procedurally* rational approach to agent selection. Key players debated and carefully calculated possible costs and benefits of lethal pathogens, eventually deciding on a mild bacterium as the final choice. It was only by luck that the group was not driven by millenarianism or an apocalyptic strategic culture, as was Aum Shinrikyo.¹²⁸ There could easily have been 751 fatal casualties at The Dalles instead of illnesses. This supports the thesis

¹²⁶ Török et al., *A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars*, 184.

¹²⁷ Ibid.

¹²⁸ Jessica Stern defines three models of terrorist motivation to use unconventional weapons. They are the rational actor model, the organizational theory model, and the strategic culture model. Rational actor and organizational theory dominated the Rajneeshee case, whereas Aum Shinrikyo, while demonstrating all three, was mostly driven by strategic culture. Stern also provides a good case study on the Aum Shinrikyo cult. See Stern, *Terrorist Motivations and Unconventional Weapons*, 205-10, 211-22.

methodology—that there is a direct link in bioterrorism between nature of attack, agent lethality, and detection and attribution (which are themselves a function of surveillance and cooperation).

Second, it demonstrates the failure of nonproliferation regimes, international and domestic security protocols, and national defense strategies to detect and deter certain types of actors and prevent low-grade BW attacks. Likewise, it also shows the difficulty in discerning signatures of BW acquisition and production—especially in the realm of non-lethal viruses, bacteria, or toxins—whether they be a product of state or non-state sponsored programs. The only signatures may be unusual spikes in human, livestock, or crop illness or death during the field testing phases shown in Figure 1 on page 22. Legitimate dual-use equipment and sensitive medical materials, the requirements of hospital labs, veterinary clinics, and research facilities, and even international trade in microbial cultures or ‘germ commerce’ all combine to aggravate an already difficult situation.¹²⁹ The Rajneesh case exemplifies the difficulty in detecting and stopping actors bent on acquiring a BW capability. Put simply, it shows we can not and will not prevent all forms of biological terrorism.

Third, and seldom if ever discussed in scholarly literature, is that the objectives of biological attacks will not always be mass casualties. The Rajneeshee case proves that to prepare only for such scenarios invites unacceptable gaps in U.S. biodefense strategy. In fact, both this case and the 2001 U.S. anthrax attacks presented in Chapter III show that objectives were not mass casualties. This is foreboding for critical infrastructure protection. The cult’s unabated success against a localized human population is very relevant today with regard to two U.S. sectors—agriculture and public health.¹³⁰ Many of the contaminated restaurants in The Dalles never recovered from the poisonings. Most

¹²⁹ There are 46 germ banks in countries as diverse as Germany, India, and Iran that stock anthrax cultures. This is according to the World Federation for Culture Collections, which is defined as a loose association of 472 specimen repositories in 61 different countries. Michael Barletta, Amy Sands, and Jonathan B. Tucker, “Keeping Track of Anthrax: The Case for a Biosecurity Convention,” *Bulletin of the Atomic Scientists* 58, no. 3 (May-June 2002): 57-62, http://www.thebulletin.org/article.php?art_ofn=mj02barletta (accessed September 20, 2006).

¹³⁰ The White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: The White House, February 2003), http://www.whitehouse.gov/pcipb/physical_strategy.pdf (accessed September 20, 2006).

lost their businesses, while others barely survived by changing names or ownership.¹³¹ Champions of critical infrastructure protection warn of bioterrorism as a tool to wage sustained economic warfare. U.S. agriculture statistics, the potential impacts on citizens and the national economy, and existing vulnerabilities all combine to present an alarming scenario.¹³²

Concerning the public health sector, its ability to absorb an attack was challenged at both state and local levels by the simple Rajneeshee salad bar contaminations. Again, had the agent used been lethal or a contagious virus, the national public health sector could have been severely crippled. The public health sector is vast and diverse, “consisting of state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles.”¹³³ The ability of this system as a whole and our first responders to survive a BW attack, provide continuity of operations, and rebound to acceptable and sustainable levels is paramount.

Finally, this case shows the importance of attribution—a tough lesson learned from poor interagency coordination during the criminal investigation which began a full year after the attacks. As mentioned in Chapter I, there are two levels of attribution: differentiating between a natural outbreak and a malicious attack, and then actually tracing back to the perpetrator. The Rajneeshee case never got past the first stage to even attempt the second. More than any other finding, this one underscores the need for effective communication and coordination between intelligence, public health, and law enforcement officials. Their relationship during the epidemiological investigation in 1984 and subsequent criminal investigation in 1985 was described as “rocky” and “a

¹³¹ Miller, Engelberg and Broad, *Germes*, 32.

¹³² U.S. agriculture accounts for one-sixth of national Gross Domestic Product which equates to over \$1 trillion a year. As a sector, it is the nation’s largest employer with one in eight working directly in food production. Exports total \$50 billion a year—the largest positive contribution to the U.S. trade balance. U.S. farming is the most efficient in the world, enabling Americans to spend less than 11 percent of disposable income on food compared to the global average of 20 to 30 percent. Parker, *Agricultural Bioterrorism*, x.

¹³³ The White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 41.

clash of cultures.”¹³⁴ Information was not shared and opportunities were missed. The lines between natural outbreak and intentional contamination were blurred, and it proved difficult to establish that a crime had been committed.¹³⁵

The Rajneeshee cult biological attacks were the first to show the vulnerability of civilian populations to chemical, biological, radiological, or nuclear terrorism.¹³⁶ Likewise, it forever changed U.S. perspectives regarding bioterrorism. It would seem this event should prompt “a realistic threat assessment based on solid empirical data,” and motivate policymakers to design “prudent and cost-effective programs for preventing or mitigating future incidents.”¹³⁷ As will be seen in the next chapter, the 2001 U.S. anthrax attacks some 17 years later confirmed that such would not be the case.

¹³⁴ Miller, Engelberg and Broad, *Germes*, 33.

¹³⁵ Ibid.

¹³⁶ Tucker, *Historical Trends Related to Bioterrorism*, 498.

¹³⁷ Ibid.

III. THE U.S. ANTHRAX ATTACKS

I do not believe science will identify the laboratory or country from which the present anthrax spores are derived. The quality of the product contained in the letter to Senator Daschle was better than that found in the Soviet, U.S., or Iraqi BW program, certainly in terms of the purity and concentration of spore particles.¹³⁸

A. INTRODUCTION

The first anthrax-laced letters were postmarked and processed through the U.S. Postal Service (USPS) on September 18, 2001. The superior quality of the spores suggested bioterrorism had reached “a new level previously viewed by many analysts...as possible, but unlikely.”¹³⁹ Widespread debate about the origin of the material used (state versus non-state source) and whether it was “weaponized” or merely pure ensued. The implications of this debate are important, because the answers shape the future bioterrorism threat environment. In this way the 2001 U.S. anthrax attacks, otherwise known as Amerithrax, signaled “a fundamental shift in the nature of the biological terrorism threat.”¹⁴⁰ This chapter analyzes the events that have spawned new legislation, government reorganization, and vast investment in biodefense infrastructure.¹⁴¹

The chapter first summarizes the case. The stresses on federal interagency coordination, the national public health system and laboratory capacity, information technology interoperability, and the control of sensitive biological materials are reviewed. Nature of attack and target selection are considered next. The incident shows how overt strikes, while more quickly detected and attributed to terrorism, still pose significant

¹³⁸ Richard Spertzel testimony before the Committee on International Relations, *Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons*, 17, http://commdocs.house.gov/committees/intlrel/hfa76481.000/hfa76481_0f.htm (accessed October 22, 2006).

¹³⁹ Parachini, *Anthrax Attacks, Biological Terrorism, and Preventive Responses*, 1.

¹⁴⁰ *Ibid.*, 17.

¹⁴¹ Examples of initiatives resulting from the 2001 U.S. anthrax attacks include but are not limited to: the *Project BioShield Act of 2004*, the *Biodefense and Pandemic Vaccine and Drug Development Act of 2006* (H.R. 5533), Homeland Security Presidential Directive/HSPD-10—*Biodefense for the 21st Century*, Projects BioWatch and BioSense, the Department of Homeland Security Science and Technology Directorate, the National Biodefense Analysis and Countermeasures Center, and enhancements for the Strategic National Stockpile and Laboratory Response Network.

national security challenges. This case illustrates that the second tier of attribution—linking attacks to a specific perpetrator—can be problematic and lengthy, if not doubtful. The agent and debate surrounding its origin and composition are also studied. Finally, the surveillance/epidemiology and detection/attribution thesis elements are considered with regard to the anthrax case. The conclusion shows four distinct findings that can be learned and applied to strengthen U.S. biodefense strategy.

B. CASE SUMMARY

The release of *Bacillus anthracis* during September through November 2001 resulted in 11 inhalational illnesses and five deaths, and the perpetrator(s) remain at large today.¹⁴² Twenty-three people were infected altogether and 62 facilities were contaminated in eight states. Aside from the obvious human toll, the attacks resulted in significant direct and indirect costs by way of decontamination efforts, unrealized future earnings, lost productivity, increased security measures, and government reorganization. The timeline of events, synopsis of contaminated facilities, and listing of the medical cases are provided in the subsequent Figures and Table.

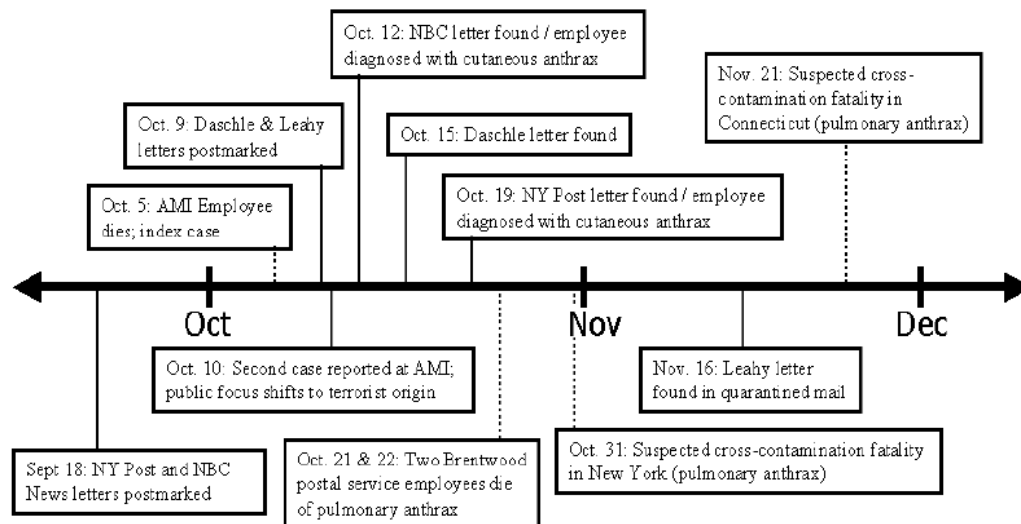


Figure 3. 2001 Anthrax Timeline. (From: *Toward a National Biodefense Strategy: Challenges and Opportunities*. Washington, D.C: Center for Counterproliferation Research, 2003, 10, <http://www.ndu.edu/centercounter/CCR%202003.pdf> (accessed December 20, 2005).)

¹⁴² Barry S. Levy and Victor W. Sidel, *Terrorism and Public Health: A Balanced Approach to Strengthening Systems and Protecting People* (New York: Oxford University Press, 2003), 105.

EPA Confirmed Anthrax-Contaminated Sites

(as of December 31, 2001)

Florida:

American Media, Incorporated, Boca Raton, FL
Two U.S. Postal Facilities, Boca Raton, FL

Three U.S. Postal Facilities, Lake Worth, FL
U.S. Postal Facility, West Palm Beach, FL

New York/New Jersey Area:

ABC News Headquarters, NY
CBS News Headquarters, NY
Manhattan Office of Governor George Pataki, NY
NBC News Headquarters, NY
New York City Hall, NY
New York Post, NY
U.S. Postal Facility, Morgan Processing Center, NY

Regional Mail Center, Hamilton Township, NJ
Mail Processing and Distribution Center, Bellmawr, NJ
U.S. Postal Facility, Rocky Hill, NJ
U.S. Postal Facility, Jackson Township, NJ
U.S. Postal Facility, Princeton Borough, NJ
Two U.S. Postal Facilities, Trenton, NJ

Washington DC Metro Area:

Brentwood Postal Facility, Washington, DC
Congressional Mail Processing Center, Washington, DC
Corporation of National Services, Washington, DC
DLA, Bolling Air Force Base, Washington, DC
Dirksen Senate Office Building, Washington, DC
Economic Research Service, USDA, Washington, DC
FBI Mailroom, Washington, DC
FCC Mailroom, Washington, DC
FDA Offices, Washington, DC
Friendship Postal Facility, Washington, DC
Hart Senate Office Building, Washington, DC
HHS Mailroom, Washington, DC
Howard University Main Mailroom, Washington, DC
Longworth House Office Building, Washington, DC
NASA, Washington, DC
OPM, Washington, DC
South Building Mailroom, USDA, Washington, DC
Three GSA Offices, Washington, DC

U.S. State Department, Washington, DC
U.S. Supreme Court Mailroom, Washington, DC
U.S. Treasury, ATF Mailroom, Washington, DC
VA Hospital Mailroom, Washington, DC
CIA Mail-Sorting Facility, Langley, VA
Dulles Retail Postal Facility, Dulles, VA
Forest Service Mailroom, USDA, Rosslyn, VA
GSA Warehouse, Alexandria, VA
Pentagon Postal Facility, Arlington, VA
FBI Mail Facility, Springfield, MD
U.S. State Department Mail-Handling Facility, Sterling, VA
Bolling Air Force Base, White House Mail Facility, MD
DOJ Mail Facility, Jessup, MD
Ford House Office Building, Washington, DC
DOJ Mail Facility, Landover, MD
U.S. Supreme Court Mail Facility, Prince Georges County, MD
Walter Reed Army Institute of Research, Silver Spring, MD

Other Areas:

Postal Machine Repair Facility, Indianapolis, IN
Stamp Fulfillment Services Building, Kansas City, MO

U.S. Postal Facility, Raleigh, NC
U.S. Postal Distribution Center, Wallingford, CT

Figure 4. 2001 Anthrax Contaminated Facilities. (From: *Observations and Lessons Learned from Anthrax Response: National Response Team Interim Report [Draft]*—October to November, 2001, 3, [http://www.nrt.org/production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/A-80anthrax/\\$File/ANTHRAX_Report_07_13_04.pdf?OpenElement](http://www.nrt.org/production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/A-80anthrax/$File/ANTHRAX_Report_07_13_04.pdf?OpenElement) (accessed November 26, 2005).)

Case	Age	Gender	Onset Date	Location	Type	Status	Source	Disp.	DOD
1	30	F	09/22/01	NYC	Cutaneous	Suspected	Sept. 18 letter	Alive	
2	38	F	09/25/01	NYC	Cutaneous	Confirmed	Sept. 18 letter	Alive	
3	39	M	09/26/01	NJ	Cutaneous	Suspected	Sept. 18 letter	Alive	
4	45	F	09/28/01*	NJ	Cutaneous	Confirmed	Sept. 18 letter	Alive	
5	63	M	09/30/01*	FL	Inhalational	Confirmed	Unfound mail	Dead	10/05/01
6	23	F	09/28/01	NYC	Cutaneous	Suspected	Sept. 18 letter	Alive	
7	73	M	09/28/01	FL	Inhalational	Confirmed	Unfound mail	Alive	
8	0.6	M	09/29/01	NYC	Cutaneous	Confirmed	Sept. 18 letter	Alive	
9	27	F	10/01/01	NYC	Cutaneous	Confirmed	Unfound mail	Alive	
10	54	M	10/13/01	NJ	Cutaneous	Removed	Oct. 9 letter	Alive	
11	56	F	10/14/01	NJ	Inhalational	Confirmed	Oct. 9 letter	Alive	
12	35	M	10/14/01	NJ	Cutaneous	Confirmed	Oct. 9 letter	Alive	
13	43	F	10/15/01	NJ	Inhalational	Confirmed	Oct. 9 letter	Alive	
14	56	M	10/16/01	DC	Inhalational	Confirmed	Oct. 9 letter	Alive	
15	55	M	10/16/01	DC	Inhalational	Confirmed	Oct. 9 letter	Dead	10/21/01
16	47	M	10/16/01	DC	Inhalational	Confirmed	Oct. 9 letter	Dead	10/22/01
17	56	M	10/16/01	DC	Inhalational	Confirmed	Oct. 9 letter	Alive	
18	51	F	10/17/01	NJ	Cutaneous	Confirmed	Oct. 9 letter	Alive	
19	34	M	10/19/01	NYC	Cutaneous	Suspected	Sept. 18 letter	Alive	
20	59	M	10/22/01	DC	Inhalational	Confirmed	Oct. 9 letter	Alive	
21	38	M	10/23/01	NYC	Cutaneous	Confirmed	Sept. 18 letter	Alive	
22	61	F	10/25/01	NYC	Inhalational	Confirmed	Unknown	Dead	10/31/01
23	94	F	11/14/01	CT	Inhalational	Confirmed	Oct. 9 letter	Dead	11/21/01
Add	?	M	3/1/02	TX	Cutaneous	Confirmed	Env. specimen	Alive	

* Originally estimated as 9/27 (case 4), and 9/27 (case 5) from media accounts but then later reported by CDC as 9/28 (case 4), and 9/30 (case 5). **CDC** = Center for Disease Control and Prevention; **MMWR** = Morbidity and Mortality Weekly Report; **Age** = years at last birthday; **gender**: M = males, F = female; **onset date**: onset of date of Anthrax signs and symptoms; **location**: NYC = New York City, NJ = New Jersey, FL = Florida, DC = Washington DC; **type**: cutaneous Anthrax and inhalational Anthrax; **status**: confirmed or suspected Anthrax (CDC definition); **source**: probable letter (postmarked date); **disp.**: disposition alive or dead; **DOD**: date of death; **add**: addenda, not part of original outbreak.

Table 3. The “Amerithrax” Medical Cases. (From: UCLA Department of Epidemiology, School of Public Health, http://www.ph.ucla.edu/epi/bioter/detect/antdetect_list.html (accessed March 1, 2006).)

The operational environment differed significantly from the 1984 Rajneeshee cult episode. First, the attacks occurred within days of the September 11th terrorist attacks and the nation was already in a heightened state of alert. Second, the anthrax attacks were overt. While no person or group claimed responsibility, the threatening letters made clear the event was not a naturally occurring outbreak from livestock or other natural source. Last, the weapon used was a high-priority Category A agent as defined by the CDC.¹⁴³ Unlike the Category B salmonella used by the Rajneeshees, anthrax can result in high mortality rates with the potential for major public health impact, can cause widespread panic and social disruption, and can require special public health actions.¹⁴⁴ Moreover, anthrax is highly stable in the environment making denial of area use, render safe, and clean up requirements arduous and costly.

While the attacks served as a wake-up call to American citizens and policymakers alike, a detailed review shows the United States was far from having a comprehensive national biodefense strategy in place despite reasonable attempts to improve preparedness after the Rajneeshee event in 1984. The *United States Government Interagency Domestic Terrorism Concept of Operations Plan* (CONPLAN) was published January 2001, just months before the attacks. The purpose of the plan was to ensure that Presidential Decision Directives 39 and 62 would be implemented in a coordinated manner.¹⁴⁵ Policymakers were beginning to acknowledge the threat of WMD terrorism, but when the first anthrax index case hit on 4 October, procedures such as the CONPLAN had not been fully implemented or exercised. A significant amount of on-the-job learning by senior government officials, public health personnel, and law enforcement officers ensued.

CDC procedures leading up to the attacks were reviewed. Initially, the United States Army Medical Research Institute of Infectious Disease (USAMRIID) forensic

¹⁴³ See <http://www.bt.cdc.gov/agent/agentlist-category.asp> for CDC explanation of agent classifications.

¹⁴⁴ National Defense University, *Toward a National Biodefense Strategy*, 30.

¹⁴⁵ The CONPLAN was the first concerted national effort to provide guidance on how the federal government would respond to terrorist threats or incidents occurring in the United States, particularly ones involving WMD. It was developed through the efforts of six primary federal departments and agencies, “consistent with...federal law, the Attorney General’s Critical Incident Response Plan...and the Federal Response Plan and its Terrorism Incident Annex.” United States Government, *CONPLAN: United States Government Interagency Domestic Terrorism Concept of Operations Plan* (Washington, D.C.: United States, 2001), iii. Also see <http://www.fas.org/irp/offdocs/pdd39.htm> for more on PDD-39, and <http://www.au.af.mil/au/awc/awcgate/ciao/62factsheet.htm> for more on PDD-39 and 62, respectively.

analysis revealed that the strain used in the attacks was one mostly used by the U.S. military and its trusted contractors.¹⁴⁶ This raised questions about the effectiveness of CDC oversight of the Select Agent Transfer Program. With the proliferation of WMD, the rise of terrorism, and the identification of over 30 new lethal pathogens in the past 20 years, Congress enacted legislation to keep tighter controls on the management of biological agents and toxins within the United States.¹⁴⁷ An amendment to the *Antiterrorism and Effective Death Penalty Act of 1996* required the Secretary of Health and Human Services (HHS) to regulate control. The CDC's Laboratory Registration/Select Agent Transfer Program was to safeguard and maintain positive control of 42 designated bacteria, viruses, and toxins. A November 2002 GAO report found the CDC's oversight left room for improvement.¹⁴⁸

Although the public health system had been preparing for biological attacks since the Rajneeshees, several diagnostic and medical treatment limitations emerged. The high demands for sample testing met with only modest capability.¹⁴⁹ The Department of Defense (DoD) provided operational support through USAMRIID. Originally designed to only assist with ten samples a month during an emergency, USAMRIID received more than 700 samples in a single day during the anthrax investigation, and surged to process more than 14,000 specimens between September 2001 and January 2002.¹⁵⁰

Other findings were that improvements in information technology could have strengthened the ability of federal agencies to respond to public health emergencies. The GAO found six key federal agencies involved in bioterrorism preparedness and response. Among these, they identified 70 systems in several information technology categories associated with public health emergency support.¹⁵¹ The main areas included detection,

¹⁴⁶ Marilyn W. Thompson, *The Killer Strain: Anthrax and a Government Exposed* (New York: Harper Collins, 2003), 14-15.

¹⁴⁷ Jon B. Woods, *USAMRIID's Medical Management of Biological Casualties Handbook*, Sixth ed. (Fort Detrick, MD: USAMRIID, April 2005), 105, <http://www.usamriid.army.mil/education/bluebookpdf/USAMRIID%20BlueBook%206th%20Edition%20-%20Sep%202006.pdf> (accessed October 25, 2006).

¹⁴⁸ General Accounting Office, *Homeland Security*, 1.

¹⁴⁹ National Defense University, *Anthrax in America*, 6.

¹⁵⁰ National Defense University, *Toward a National Biodefense Strategy*, 41.

¹⁵¹ General Accounting Office, *Bioterrorism*, 1.

surveillance, communication, and support technologies. The report found interoperability to be a serious problem. During the outbreak, Senator Fred Thompson said, “The good news is that there are many agencies working on all of these issues. The bad news is that there are many federal agencies working on all these issues.”¹⁵²

U.S. consequence management of Amerithrax exposes the nation’s level of preparedness for biodefense. The impact would have been greatly magnified had the crisis not occurred when it did, and if it had not been overt in nature. Following the September 11th attacks America was more alert to the possibility of terrorist acts. Moreover, it would have taken longer to detect and attribute the event had the attacks been covert. Even so, the shortcomings of federal jurisdiction and public health and law enforcement integration—from who was in charge, to protecting the chain of evidence, to attribution—were all critically exposed as a result of the U.S. anthrax attacks.¹⁵³ These deficiencies may have contributed to why the perpetrator(s) remain unidentified and at large today.

C. NATURE OF ATTACK AND TARGET

The anthrax attacks were overt. Regardless of the actor(s), their intent, or the lack of any claimed responsibility, the written message broadcasting the assault made the situation clear. Four letters were recovered, although some believe as many as seven may have been mailed.¹⁵⁴ The FBI believes they were sent in two distinct waves. The first wave was postmarked 18 September and may have included one to America Media, Inc. (AMI) in Florida (not recovered), one to *The New York Post* (recovered), one to NBC (recovered), one to CBS (not recovered), and one to ABC (not recovered) in New York. The second wave was postmarked 9 October and consisted of the Senators Tom Daschle and Patrick Leahy letters, both of which were recovered.¹⁵⁵ All were originally believed

¹⁵² Quoted in National Defense University, *Anthrax in America*, 3.

¹⁵³ DOL/OSHA and U.S. Coast Guard (USCG) took lead roles in the response. The USCG Atlantic Strike Team established and staffed the Incident Command System/Unified Command structure for the Capitol Hill response. Often agencies were confused on which federal plan should be activated or who had jurisdiction in different buildings. See National Response Team, *Observations and Lessons Learned from Anthrax Response: National Response Team Interim Report [Draft] - October to November, 2001*, 5-7, [http://www.nrt.org/production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/A-80anthrax/\\$File/ANTHRAX_Report_07_13_04.pdf?OpenElement](http://www.nrt.org/production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/A-80anthrax/$File/ANTHRAX_Report_07_13_04.pdf?OpenElement) (accessed November 27, 2005).

¹⁵⁴ National Defense University, *Anthrax in America*, 5.

¹⁵⁵ Ibid.

to contain one of the variants of the Ames strain, and the quality of the samples varied. While some were crude, the spores in the letters sent to Senators Daschle and Leahy were under five microns in diameter and were also of extremely high concentration and purity.¹⁵⁶

Fortunately, it appears the distribution was not intended to produce mass casualties, but rather to send a signal of sorts. Georgia State University professor and terrorism expert Jack Williams said, “I think this is a distraction, a form of disruption. They know us pretty well, how we will react, ...and if Osama bin Laden is involved, it is part of an overall, long-haul approach.”¹⁵⁷ Former Central Intelligence Agency (CIA) counterterrorism official Vincent Cannistraro explained, “It just doesn’t have the fingerprints or the pattern of a bin Laden operation. Al Qaeda wants to inflict mass casualties and kill as many people as they can. Sending individual, targeted mailings is not going to accomplish that...”¹⁵⁸

While it is difficult to know for sure, it is noteworthy that the first letters were all sent to journalists and media outlets. This suggests a desire to maximize public exposure of the event and incite widespread panic. Also noteworthy is that this batch contained the less potent material. The second wave, containing the more refined and deadly spores, were sent to leaders of U.S. government. An objective here may have been to demonstrate the U.S. government’s inability to protect itself, let alone the American public. Senator Michael Crapo said the Daschle letter was essentially an assassination attempt on a government leader. “There’s no other way to put it: It’s an attack on the government.”¹⁵⁹ Regardless, experts believe the direct mailings versus a public aerosol release or other mass delivery method indicate the goal was not mass casualties. Former Soviet bioweapons engineer Dr. Kenneth Alibek concluded “...it was not an actual

¹⁵⁶ Milton Leitenberg, *Biological Weapons and “Bioterrorism” in the First Years of the 21st Century* (College Park, MD: Center for International and Security Studies, School of Public Affairs, April 2003), 40-41.

¹⁵⁷ Quoted in National Defense University, *Anthrax in America*, 39.

¹⁵⁸ *Ibid.*, 34.

¹⁵⁹ *Ibid.*, 33.

biological weapon attack, it was a psychological economic attack using biological agents.”¹⁶⁰ The objectives were to create a national panic and marginalize the government’s ability to protect its citizens.

The mechanics of USPS processing machines, however, did cause exposure to postal workers as well as cross-contamination of mail. The Daschle letter contaminated the Brentwood processing facility. Law enforcement officials found that the letter left “a trail of spores as it passed through automated, high-speed mail sorting equipment, and tests consistently found spores along the precise path taken by the Daschle letter...”¹⁶¹ It is uncertain whether this was an intended consequence. Nineteen buildings or facilities in the Washington, D.C. area possessed levels of contamination described as “medically insignificant and too small to lead to human infection.”¹⁶² All Senate and House buildings were closed for assessment, and the House adjourned for the week while the Senate remained defiantly in session.¹⁶³ The Hart Office Building remained quarantined for months until decontaminated.

D. AGENT CONTROVERSY

1. Anthrax and Its Potential Impact

Bacillus anthracis is a bacterium that forms spores—a cell that is dormant but may come to life under the right conditions. It may present in one of three forms: on the skin (cutaneous), in the lungs (inhalation), or in the digestive system (gastrointestinal).¹⁶⁴ An aerosol dissemination is the most effective way to inflict casualties. From the perspective of biological warfare, a cloud or “line” of anthrax laid from an aerial vehicle “should consist of particles of one to five microns (one-millionth of a meter) in size.”¹⁶⁵ The upper respiratory track removes larger particles and prevents them from penetrating

¹⁶⁰ Kenneth Alibek testimony before the Committee on International Relations, *Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons*, 69.

¹⁶¹ *Ibid.*, 44.

¹⁶² Leitenberg, *Biological Weapons and “Bioterrorism,”* 41.

¹⁶³ National Defense University, *Anthrax in America*, 35.

¹⁶⁴ Department of Health and Human Services, “Anthrax: What You Need to Know,” Centers for Disease Control and Prevention, <http://www.bt.cdc.gov/agent/anthrax/needtoknow.asp> (accessed February 28, 2006).

¹⁶⁵ W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit use of Biological Agents since 1900* (Washington, D.C.: National Defense University, February 2001), 17-18, http://www.ndu.edu/centercounter/Full_Doc.pdf (accessed December 7, 2006).

the lungs. Particles larger than five microns settle from the atmosphere too quickly to be effective. Particles smaller than one micron are breathed out and do not persist in the lungs.¹⁶⁶

Aerosol deliveries are of concern because many diseases are most dangerous when contracted in this manner.¹⁶⁷ For example, when cutaneous anthrax is contracted through the skin the case fatality rate is five to 20 percent, although antibiotics are highly effective. In contrast, pulmonary or inhalation anthrax is usually fatal and if not detected early there is no useful treatment.¹⁶⁸ Theoretically, 100 kg of anthrax spores spread over Washington, D.C. could kill one to three million people if disseminated effectively and during the right environmental conditions.¹⁶⁹ The World Health Organization estimates that 50 kg of agent used on a city of one million people would kill 36,000 and incapacitate another 54,000 persons.¹⁷⁰

In *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, Seth Carus mentions 33 cases of non-state involvement in the acquisition of biological agents. He points to four different acquisition methods that were used. These include purchase from legitimate suppliers, theft, self-production, and use of natural materials contaminated with biological agents.¹⁷¹ “Gaining access to biological agents never appears to have been a significant limiting factor. In fact, acquiring biological agents has usually proven to be relatively easy.”¹⁷² If this is true, then it opens the door and adds weight to the argument of a non-state connection to the 2001 anthrax attacks.

2. State versus Non-State Connection

Widespread debate focused on the exact characteristics of the pathogen used. Disagreement began within days of the attack and continues today some five years later. The composition of the agent is important, because its level of sophistication can point to

¹⁶⁶ Carus, *Bioterrorism and Biocrimes*, 17-18.

¹⁶⁷ Ibid.

¹⁶⁸ Ibid.

¹⁶⁹ From the U.S. Congress Office of Technology Assessment report, *Proliferation of Weapons of Mass Destruction: Assessing the Risks*. Ibid., 17.

¹⁷⁰ Ibid., 18.

¹⁷¹ Ibid., 13-15.

¹⁷² Ibid., 13.

either state-sponsorship or possibly a non-state actor source. Initial suspicion focused on a state actor such as Iraq, or the sub-national terror group Al Qaeda, especially since the letters were posted one week to the day following the September 11th attacks.¹⁷³ Richard Butler, former Chairman of the United Nations Special Commission (UNSCOM) said the anthrax sent to Senator Daschle's office was very potent and small in particle size. Four weeks into the crisis he was convinced that the agent did not come from amateurs. "The two candidates for immediate investigation, I think would be Iraq and Russia...", he said.¹⁷⁴ Richard Spertzel, consultant and former chief UNSCOM biological weapons inspector commented on the quality of the anthrax sent to Senator Daschle's office saying, "It tells me that this is no homegrown terrorist. This indicates a foreign source of knowledge at least."¹⁷⁵ A myriad of others would disagree with these initial claims.

On 8 October, just three weeks after the initial wave of letters, Dr. D.A. Henderson of the Johns Hopkins University Center for Civilian Biodefense Studies said, "It is certainly not an engineered strain, not a strain like the Russians produced and wrote about. They said they had produced an antibiotic resistant strain."¹⁷⁶ Dr. Scott Lillibridge, Special Assistant to the HHS Secretary for Bioterrorism noted the initial Florida strain was sensitive to penicillin and a variety of other drugs. "This is not the hallmark of an engineered bio-weapon," he explained.¹⁷⁷ More doubts about state involvement surfaced the following week. Major General John Parker of the U.S. Army Medical Research and Material Command said the anthrax tested from the Daschle letter was pure, but represented a common variety not genetically engineered. CDC spokesperson Lisa Swenarski stated it was a natural strain responsive to all antibiotics available to treat anthrax. USAMRIID spokesperson Caree Vander Linden explained, "There is no evidence that this is engineered to be more potent than [sic] the naturally occurring form of anthrax."¹⁷⁸ Finally, on 18 October Senator Rick Santorum tried to

¹⁷³ National Defense University, *Anthrax in America*, 8.

¹⁷⁴ Quoted in National Defense University, *Anthrax in America*, 38.

¹⁷⁵ Ibid.

¹⁷⁶ Ibid., 24.

¹⁷⁷ Ibid., 27.

¹⁷⁸ Ibid., 36.

calm public fears by saying, “My understanding is that this strain of anthrax...responded to every antibiotic used against it, even 1943 penicillin. Everyone needs to understand that this is a threat we have a response for.”¹⁷⁹

The most convincing arguments against a state-sponsored link come from Dr. Kanatjan Alibekov (Kenneth Alibek), the former first Deputy Director of Biopreparat in the Soviet Union.¹⁸⁰ On 5 December and before the Committee on International Relations, Dr. Alibek presented his argument why the anthrax was not the product of a state biological weapons program:

Talking about anthrax, I know something about this powder sent to different locations. ...my first conclusion is that I am convinced this agent and this product cannot be considered as a Russian or an American weapon. ... What I haven't seen is the fine particle size. Yes, some of this formulation was in fine particle size. But there are many particles which were a larger size. My analysis shows that this product was not obtained using either American or Russian production techniques.¹⁸¹

He elaborated on the wide distribution of particles size. Some were very small, on the order of one, two, three, five, and ten microns in diameter, while others were larger measuring up to 35 or 50 microns.¹⁸² Electron microscopy was used to examine particle form to see if a highly technical milling process was applied. Alibek claimed he did not see evidence of such a process.¹⁸³ His third point was that the sophistication level of the batches were different. The first product was not superior and contained vegetative cells or immature spores, whereas the later material was higher quality and much more pure. To Alibek, this showed learning in the process of manufacturing—a certain sign of non-

¹⁷⁹ Quoted in National Defense University, *Anthrax in America*, 40.

¹⁸⁰ Dr. Kenneth Alibek was born in Kazakhstan. During his years with Biopreparat developing the world's deadliest biological agents for the Soviet Union, Alibek and his colleagues assumed the United States was developing the same weapons. He discovered that the United States, unlike the Soviet Union, was abiding by an agreement not to develop biological weapons during a trip to inspect American facilities. Realizing this, he defected to the United States in 1992 and provided officials with details of the Soviet Union's biological weapons programs. He currently conducts research in Manassas, Virginia to enhance the general immune system against bioweapons exposure. Internet Movie Database, “Biography for Ken Alibek,” <http://www.imdb.com/name/nm1985907/bio> (accessed October 22, 2006).

¹⁸¹ Alibek, *Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons*, 22-23.

¹⁸² *Ibid.*, 23.

¹⁸³ *Ibid.*, 24.

state involvement.¹⁸⁴ U.S. Surgeon General David Satcher supported Dr. Alibek and others' claims of a non-state sponsored source. Commenting on the strains from Florida, New York, and Washington, D.C., Satcher said the bacteria was not produced in a "weaponized" form.¹⁸⁵ Thirty-one genetic markers matched in the anthrax from these different locations, meaning they were from the same stock material. The particles were of different size, but the underlying strain was the same. Satcher, like many others, held it to be a "naturally occurring" strain.¹⁸⁶

Debate also centered on whether the anthrax was the Ames strain. Ames became available in U.S. biodefense programs in the early 1980s, and was the standard used to develop new vaccines because of its potency. On 10 October, *The Miami Herald* reported that investigators linked the agent used to anthrax harvested in Iowa in the 1950s.¹⁸⁷ Later that evening, an *NBC News* report implied the FBI thought it was stolen from a Department of Energy laboratory in Ames, Iowa.¹⁸⁸ Nonetheless, Dr. Martin Hugh-Jones of Louisiana State University insisted, "It's not the Ames strain, far from it."¹⁸⁹ Richard Spertzel echoed this view saying it was not an identical match to the Ames strain.¹⁹⁰ However, on 13 October *Newsday* reported that a team of microbiologists from Lawrence Livermore National Laboratory tested the Florida sample. The scientists found that despite previous denials from health officials, it was indeed the Ames strain developed in the 1950s.¹⁹¹ Five to 20 laboratories in the United States, the United Kingdom, Canada, and probably Israel have possessed or worked with Ames. As a result, efforts were taken to identify the different genomes linked to its use in these laboratories.¹⁹² Dugway Proving Grounds, Utah was a major production facility in the U.S. biodefense program. Dugway also produced dry powder versions and weapons-

¹⁸⁴ Alibek, *Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons*, 24.

¹⁸⁵ National Defense University, *Anthrax in America*, 41.

¹⁸⁶ *Ibid.*

¹⁸⁷ *Ibid.*, 26.

¹⁸⁸ *Ibid.*

¹⁸⁹ Quoted in National Defense University, *Anthrax in America*, 27.

¹⁹⁰ *Ibid.*, 30.

¹⁹¹ *Ibid.*

¹⁹² Leitenberg, *Biological Weapons and "Bioterrorism,"* 41.

grade anthrax. It is known that at least one U.S. contractor for the CIA worked with the strain, but “allegedly had made no dry powder.”¹⁹³ Most scientific experts and investigators today believe the Ames strain was used in the attacks.

Recently on September 25, 2006, the FBI extended its search of suspects to include those not connected or having access to the defense establishment.¹⁹⁴ FBI Hazardous Materials Response Unit scientist Douglas Beecher said, “A widely circulated misconception is that the spores were produced using additives and sophisticated engineering supposedly akin to military weapons production.”¹⁹⁵ Whoever produced the anthrax achieved extraordinary purity and quality (up to a trillion spores per gram), but used none of the techniques known to military BW scientists.¹⁹⁶ “It wasn’t weaponized. It was just nicely cleaned up,” said one scientist who spoke anonymously because of the ongoing investigation. “Whoever did it was proud of their biology. They grew the spores, spun them down, cleaned up the debris. But there were no additives.”¹⁹⁷

3. “Weaponized” versus “Pure”

The difference between a weaponized and pure agent deserves mention. Even today as back then, the two terms are often misused as one in the same. On 17 October, HHS Secretary Tommy Thompson claimed the anthrax was weapons grade during a congressional hearing. He said it was pure, requiring the significant resources of a country, but later added that “a well-financed terrorist group” could also have sufficient resources to do the job.¹⁹⁸ Later on 23 October, Representative Richard Gephardt described the agent as “weapons grade” because of its sophisticated small particle size and ability to aerosolize.¹⁹⁹ However, where biological weapons are concerned, purity alone does not necessarily mean weaponization.

¹⁹³ Leitenberg, *Biological Weapons and “Bioterrorism,”* 44.

¹⁹⁴ Allan Lengel and Joby Warrick, “FBI Is Casting A Wider Net in Anthrax Attacks,” *Washingtonpost.com*, <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/24/AR2006092401014.html> (accessed October 5, 2006).

¹⁹⁵ Quoted in Lengel and Warrick, *FBI Is Casting A Wider Net in Anthrax Attacks*.

¹⁹⁶ *Ibid.*

¹⁹⁷ Quoted in Lengel and Warrick, *FBI Is Casting A Wider Net in Anthrax Attacks*.

¹⁹⁸ National Defense University, *Anthrax in America*, 37.

¹⁹⁹ *Ibid.*, 44.

The literature points to a weaponized agent as meaning one traditionally engineered by state programs. Dr. Kenneth Alibek and UNSCOM inspector Richard Spertzel would characterize these as pathogens that have not only been milled to fine particle size, but that also have special additives or coatings applied to resist antibiotics or other medical countermeasures. These are the subtle signatures of true weaponization, which traditionally have been the exclusive realm of a select few states. Nevertheless, it also stands to reason that any pathogen altered from its natural form for the purposes of causing illness or death would also be considered a weapon in the traditional sense.

Whether weaponized or pure, the real question is does it matter regarding the needs of a comprehensive national biodefense policy. Findings from the Rajneesh case presented earlier, and the surveillance and cooperation limitations that hamper detection and attribution capabilities presented in the next chapter, prove that it does not matter. Whether weaponized or pure, whether salmonella or anthrax, and whether covert or overt, a comprehensive national biodefense policy requires looking beyond these debates.

E. SURVEILLANCE AND EPIDEMIOLOGY

Pulmonary anthrax is extremely rare in the United States. The replacement of goat hair with synthetic substitute fibers all but eliminated the primary source of exposures. Prior to the attacks, there were only 18 reported cases of inhalational anthrax between 1900 and 1978, and none from then until 2001.²⁰⁰ On 4 October, Florida Department of Health Secretary Dr. John Agwuboni announced that AMI tabloid editor Robert Stevens had been diagnosed with pulmonary anthrax. This was the first such case in the United States in 25 years.²⁰¹ CDC and state health departments immediately responded to boost surveillance efforts. “We have strengthened our surveillance system in order to give us any early warning signs of an illness or a cluster of illnesses that would suggest exposure to a bioterrorist agent,” explained New York Department of Health Commissioner Dr. Neal Cohen.²⁰² Bulletins clarifying the symptoms and

²⁰⁰ National Defense University, *Anthrax in America*, 9.

²⁰¹ *Ibid.*, 20.

²⁰² Quoted in National Defense University, *Anthrax in America*, 25.

treatment for anthrax were faxed to 65,000 doctors in New York, as well as further bioterror instructions to first responders and other care providers in accordance with state plans.²⁰³

Two of Robert Steven's coworkers also fell ill and spores were found throughout the AMI building. On 12 October, it was announced that an assistant to Tom Brokaw of *NBC News* had contracted cutaneous anthrax after opening a letter postmarked from Florida.²⁰⁴ Days later a personal assistant to Dan Rather of *CBS News* was also diagnosed with cutaneous anthrax after opening a suspicious letter. Investigators found spores at several facilities throughout New York including the second floor mailroom at *ABC News*, the Manhattan office of New York Governor George Pataki, New York City Hall, the *New York Post*, and the USPS Morgan Processing and Distribution Center. Spores were also found in mail facilities throughout New Jersey including Trenton, Jackson Township, Hamilton Township, Rocky Hill, and Princeton Borough. Exposure of postal workers resulted in two cases of inhalation anthrax and three of the cutaneous form.²⁰⁵ By mid-October the crisis had reached Washington, D.C. A letter was opened in the office of Senator Daschle resulting in the evacuation and closure of congressional office buildings, as well as stopping almost all federal mail deliveries in the National Capital Region.²⁰⁶

Over a period of eight weeks, the attacks produced 22 confirmed cases and five deaths.²⁰⁷ Case number 16 (Table 3, page 42) was Joseph Curseen, a 47-year-old postal worker of the Brentwood USPS facility. On 16 October (day one of onset), he developed nausea, abdominal pain, and "flu-like" symptoms, but attributed these to food poisoning.²⁰⁸ On 21 October (day six), he reported to work for the night shift with worsening symptoms and eventually drove himself to the emergency room at Southern

²⁰³ National Defense University, *Anthrax in America*, 25.

²⁰⁴ National Response Team, *Observations and Lessons Learned*, 2.

²⁰⁵ Ibid.

²⁰⁶ National Defense University, *Anthrax in America*, 5.

²⁰⁷ Leitenberg, *Biological Weapons and "Bioterrorism,"* 40-41.

²⁰⁸ Luciana Borio et al., "Death Due to Bioterrorism-Related Inhalational Anthrax: Report of Two Patients," *The Journal of the American Medical Association* 286, no. 20 (November 28, 2001), 2554-2556, <http://www.ph.ucla.edu/epi/bioter/joc11802.pdf> (accessed March 1, 2006).

Maryland Hospital Center at 2:00 AM.²⁰⁹ “After treatment with intravenous fluids, promethazine, and famotidine his symptoms resolved... He was discharged to home at 5:00 AM with a presumptive diagnosis of gastroenteritis and instructions to see his primary care physician the following day.”²¹⁰ The next morning at 4:45 AM his wife found him slumped in the bathroom and he was taken to the hospital by ambulance. Five hours after admission on day seven, Mr. Curseen died.

On the whole, hospital physicians and staffs responded well during the crisis. Yet this victim’s medical case stands out as a failure among successes with regard to surveillance. The widow of Mr. Curseen filed suit against hospital staff for misdiagnosis, claiming doctors failed to detect the anthrax during his first visit even though several other cases from Brentwood and elsewhere had been linked to the mail. Charges also allege that Curseen told emergency room workers he was employed at Brentwood, and that this information also appeared on his charts. Even so, his blood was not tested and he did not receive other measures that could have detected the illness and saved his life.²¹¹

On 3 October and only several days into the crisis, HHS Secretary Thompson testified before the Senate Subcommittee on Labor, Health, and Human Services. Regarding bioterror response plans, he acknowledged that shortfalls existed with national laboratory capacity and the education of our health force concerning the clinical signs of BW attacks.²¹² Former Soviet bioweapon engineer Dr. Kenneth Alibek shared these concerns when he said, “We are underprepared. Most doctors and nurses have never seen such cases. They have no idea how to diagnose these infections.”²¹³ In sum, the U.S. anthrax attacks “tragically confirmed the importance of disease surveillance, since the speed with which doctors recognized the signs of anthrax infection determined whether patients were treated immediately or sent home, only to return later to die.”²¹⁴ U.S.

²⁰⁹ Stephen Manning, “Hospital Sued by Family of Anthrax Victim,” *Baltimore Sun*, <http://www.ph.ucla.edu/epi/bioter/hospitalsued.html> (accessed March 1, 2006).

²¹⁰ Quoted in Borio et al., *Death due to Bioterrorism-Related Inhalational Anthrax*.

²¹¹ Manning, *Hospital Sued by Family of Anthrax Victim*.

²¹² National Defense University, *Anthrax in America*, 20.

²¹³ *Ibid.*, 23.

²¹⁴ Chyba, *Toward Biological Security*, 131.

consequence management of this event highlights the significance of improving domestic defenses, especially since “many tools used to address natural disease threats will be needed to respond to an intentional attack.”²¹⁵

F. DETECTION AND ATTRIBUTION

1. “Anthrax Happens”²¹⁶

Government officials and agency experts moved to abate public fears the same day Robert Stevens was diagnosed with the first U.S. case of pulmonary anthrax in 25 years.²¹⁷ Secretary Thompson mentioned that Stevens drank from a stream in North Carolina while traveling the week prior, and insisted there was no evidence pointing to terrorism. CDC Director Dr. Jeffrey Koplan emphasized that Stevens was an isolated case, and urged people not to panic and stockpile or use antibiotics. The FBI issued public statements saying there was no preliminary evidence indicating his illness was related to criminal activity. “The FBI is assisting health officials in searches, but at this point investigators are conducting a public health probe, not a criminal investigation,” explained FBI spokesperson Judy Orihuela.²¹⁸ The government position in early October was clearly one of calming fears, preventing panic, and resisting the notion of conjecture.

2. Suspicions Rise

Authorities in Florida eliminated natural causes as the source of anthrax the same day letters were postmarked to Senators Daschle and Leahy in Trenton, New Jersey.²¹⁹ Multiple infections of such a rare type in such a short period of time made natural causes for the outbreaks seem implausible. Candid views were reflected in statements such as: “Unless this guy was sniffing sheep’s wool for a living, and if it is inhalational anthrax, that is enough to raise the alarm;” and “Somebody definitely had to introduce it into the office; it couldn’t walk in by itself.”²²⁰ Consultant and former UNSCOM inspector

²¹⁵ Chyba, *Toward Biological Security*, 122.

²¹⁶ In an effort to alleviate public fear on October 4, 2001, North Carolina Department of Public Health spokesperson Debbie Crane said, “Anthrax happens. It’s happened forever, and it’s happened before Sept. 11.” National Defense University, *Anthrax in America*, 21.

²¹⁷ *Ibid.*, 20-21.

²¹⁸ Quoted in National Defense University, *Anthrax in America*, 22.

²¹⁹ *Ibid.*, 24.

²²⁰ The first quote is from Dr. Michael Asher, Director of the California infectious disease laboratory on 8 October. The second is from Jeanne Kwik of the Johns Hopkins University Center for Civilian Biodefense Studies on 10 October. *Ibid.*, 23, 27.

Richard Spertzel also said on 9 October, “I do not believe that it was accidental. ... You do not expect to find anthrax floating around the air in buildings in a city or even on a farm—it’s not a natural event.”²²¹ Congressman Porter Goss described the agent and its implications, noting that the signs of professionalism reflected in its quality point to signs of organization. “We’re dealing with something that was targeted [and] reasoned. The methods were not haphazard...”²²² The definitive sign of the anthrax outbreaks being attributed to terrorism, however, came from a swift change in public statements by Secretary Thompson. On 12 October he insisted there is “no proof whatsoever” that the *NBC News* exposure was terrorism, saying it was an “unusual occurrence” and asking reporters to “...resist the urge to speculate.”²²³ Just two days later on *CNN* he said, “There’s no question it’s bioterrorism. It’s a biological agent. It’s terrorism, it’s a crime... But whether or not it’s connected to al-Qaida, we can’t say conclusively,”²²⁴

3. Challenges of Coordination

Awareness that infections stemmed from a deliberate act turned what started out as a public health response into a law enforcement investigation. On 10 October, Florida U.S. Attorney General Guy Lewis confirmed this by stating “It’s now a criminal investigation.”²²⁵ Officers interviewed workers of government and academic laboratories who may have had access to anthrax.²²⁶ Polygraphs were administered and homes were searched. The FBI defends its investigative methods as being systematic and thorough. Yet the agency has been criticized for not consulting proper bioterrorism and biotechnology experts until months into the investigation. “There was a delay of several months before the FBI subpoenaed laboratories working with the Ames strain of anthrax, requesting samples for testing and comparison.”²²⁷ On 9 October Attorney General John Ashcroft said, “We are relying on the Centers for Disease Control and health authorities

²²¹ Quoted in National Defense University, *Anthrax in America*, 25.

²²² *Ibid.*, 37.

²²³ *Ibid.*, 28.

²²⁴ *Ibid.*, 31.

²²⁵ *Ibid.*, 26.

²²⁶ *Ibid.*, 8.

²²⁷ *Ibid.*, 9.

to provide expertise which we do not have. Very frankly, we are unable to make a conclusive statement about the nature of this as either an attack or an occurrence, absent more definitive laboratory and other investigative returns.”²²⁸

New forensic methods were developed “to balance legal evidentiary needs against scientific and public health requirements.”²²⁹ Four letters were recovered by law enforcement personnel.²³⁰ EPA and FBI criminal investigation hazardous material teams searched 280 barrels containing 635 bags of quarantined mail that had been seized as evidence. The final letter was addressed to Senator Leahy. It was found on 16 November, approximately two-thirds into the very last bag searched.²³¹

Dr. Kenneth Alibek’s congressional testimony epitomized the difficulties and requirements for interagency coordination to effect attribution of BW attacks. Whereas the Attorney General said law enforcement was relying on the CDC and health experts to fill investigative gaps, Dr. Alibek pointed to the need for law enforcement to assist scientists.

Just by analyzing this product, you cannot answer this question [of actor]. It would require additional study by some experts from completely different fields. Psychology or the FBI probably would be the best sources to determine who could make this product.²³²

It became immediately clear that the 2001 U.S. anthrax attacks ushered in the need for a new level of coordination if attribution was to occur.

G. CASE FINDINGS

Four distinct findings can be drawn from this case to strengthen U.S. biodefense strategy. The crisis carried a monumental cost in terms of disruption.²³³ Several congressional office buildings were closed for months following the attacks. The AMI building in Florida and USPS facilities in Washington, D.C., New Jersey, and

²²⁸ Quoted in National Defense University, *Anthrax in America*, 25.

²²⁹ Ibid.

²³⁰ Ibid., 5.

²³¹ See Federal Bureau of Investigation, *Amerithrax*, for a complete account of the FBI-EPA investigative protocols used during the search.

²³² Alibek, *Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons*, 24.

²³³ National Defense University, *Anthrax in America*, 6.

Connecticut remained closed for more than a year. The Hart Office Building remained quarantined for 96 days. The EPA estimated it alone had spent \$13.3 million on clean up for this building, and expected their total costs to rise above \$20 million.²³⁴ It should be noted these figures represent funds from only one federal agency's budget, for merely one building, and from just one BW attack. This case illustrates the costly long-term effects to government and society from a relatively simple one-off attack.

Second, this case demonstrates that determined actors—whether state-sponsored, sub-national, domestic, or lone-wolf—will not relent in their quest to successfully produce biological weapons. They are aptly maneuvering through or around the four necessary capabilities mentioned in Chapter I. Scientific consensus that the agent was not “weaponized” in the traditional sense, yet achieved sophistication and exceptional purity on par with state BW programs shows that would-be terrorist are gaining ground. This brings into question the limitations of nonproliferation and domestic and international security protocols to prevent acquisition of sensitive materials. To prevent access, countries and international organizations must first have detailed knowledge of who has what—a daunting task considering legal reporting requirements and the multitude of government, academic, and private sector laboratories and germ banks with pathogens.

Third, detection of the attacks through medical surveillance proved to be limited. In several instances physicians misdiagnosed both cutaneous and pulmonary anthrax. The initial Florida cases of Robert Stevens and Ernest Blanco were originally diagnosed as pneumonia.²³⁵ The Florida Department of Health laboratory did, however, provide quick and accurate identification of anthrax. This was due to technicians who had recently completed a Laboratory Response Network (LRN) training course funded with bioterrorism response money.²³⁶ Another surveillance limitation concerned laboratory surge capacity during a BW attack. Complicating the already heavy demands were an enormous number of hoaxes and false alarms following the actual events. According to CDC statistics, its laboratories and that of the LRN tested over 125,000 samples after the

²³⁴ National Defense University, *Toward a National Biodefense Strategy*, 93.

²³⁵ National Defense University, *Anthrax in America*, 9.

²³⁶ Ibid.

first reports of outbreak. Laboratories were so overwhelmed, they considered creating ad hoc triage schemes to prioritize tests.²³⁷ The primary lesson for improved detection through surveillance was increased education for clinicians and first responders to identify signs of bioterrorism, and increased laboratory surge capacity. However, even when these improvements do yield fruit, medical and public health systems must interface with law enforcement and other outside agencies in order to help. A frustrated AMI employee summed it this way: “It took five days to figure out this anthrax was in the building. If this is how quickly you diagnose something like this, we’re in trouble.”²³⁸

Last, and more than any other case, Amerithrax provides a glimpse into the future of countering bioterrorism, which is robust and reliable attribution.

A viable strategy and improved tool kit to rapidly and accurately attribute bioterror attacks [is needed]. Absent a clear, unambiguous ability to determine complicity in bioterror events, the nation’s ability to effectively deter future perpetrators is in jeopardy.²³⁹

Implicit in the ‘improved tool kit’ for attribution is the need for improved interagency coordination. They are simply indivisible. Likewise, Amerithrax marked the beginning of special investigative protocols between medical, public health, environmental, and law enforcement communities. It highlighted infrastructure shortfalls that prompted today’s biodefense initiatives including Projects BioShield, BioWatch, and BioSense; refinements in the Strategic National Stockpile and Laboratory Response Network, and creation of the National Biological Analysis and Countermeasures Center.

The Salmonella contamination of food by the Rajneeshee cult in 1984 and response to the anthrax attacks of 2001 are informative case studies. This is because they reveal a relationship of independent variables that influence the likelihood of BW detection and attribution. The first was a *covert* attack using a *non-lethal* agent that resulted in *many* victims, while the second was an *overt* attack using a *lethal* agent that resulted in *few* casualties. While the perpetrators of the covert Salmonella attack were

²³⁷ National Defense University, *Anthrax in America*, 10.

²³⁸ *Ibid.*, 26.

²³⁹ *Ibid.*, 16.

caught and imprisoned, the terrorist(s) in the overt anthrax attack remain at large. These relationships form a notional model of biodefense that is considered in Chapter IV. Previous U.S. methods to deal with the threat of bioterrorism have focused on nonproliferation, counterproliferation, and state actors. These methods failed to prevent both the Rajneeshee and anthrax cases. Today's environment requires a capabilities-based approach independent of the nature of the actor. The findings from these two cases are now compared to current biodefense initiatives. The resulting gaps will lead to policy recommendations provided in Chapter V to shore up U.S. biodefense strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TOWARD DETECTION AND ATTRIBUTION

We ought to assume that there's been some coordination.²⁴⁰

The thesis has examined two informative case studies up to this point, and has identified limitations that diminish biodefense and overall national preparedness for BW attacks. This chapter synthesizes the findings and makes a case for the primacy of detection and attribution. Rapid detection and attribution capabilities are absolutely critical to success. They are the vital elements of a comprehensive national biodefense policy that will increase preparedness for either naturally occurring disease or malicious biological attacks.

The chapter begins by defining detection and attribution in terms of biodefense, and is organized in five sections. First, this chapter compares the Rajneesh and anthrax cases to demonstrate a need for these critical capabilities. Second, it provides a notional model of biodefense based on findings from these cases. Third, this chapter calls for a re-balancing of national biodefense priorities from current infrastructure expenditures to basic organizational improvements in order to bolster detection and attribution. Fourth, it considers current public health limitations and their effect on detection through surveillance. Last, the chapter examines nature of attack, surveillance and epidemiology, and the emerging field of forensic epidemiology to better understand how establishing collaborative networks can improve interagency cooperation so that attribution can be achieved.

A note about what this chapter does not cover: the response phase or consequence management of biological events. The medical system comprised of for-profit hospitals, clinics, and Health Management Organizations is distinctly different and altogether separate from the U.S. public health system.²⁴¹ The ability of the medical system—based on business models and just-in-time medical care—to surge and provide adequate

²⁴⁰ Statement of Senator Ted Kennedy in response to developments in the U.S. anthrax attacks on October 14, 2001. This was the day a New York City Police Department officer and two New York City laboratory technicians tested positive for anthrax from handling the NBC letter. It was also on this date that HHS Secretary Thompson first publicly attributed the attacks to bioterrorism. National Defense University, *Anthrax in America*, 33.

²⁴¹ Sarah A. Lister, *An Overview of the U.S. Public Health System in the Context of Emergency Preparedness* (Washington, D.C.: Congressional Research Service, March 17, 2005).

services during response to BW attacks are not examined.²⁴² Rather, the emphasis is on the U.S. public health system, the elements within it that form limitations, and the overall effect on national detection through surveillance. When response is discussed, it will be in relation to what facets of detection and attribution can facilitate the transition to effective response.

Detection occurs when public health officials differentiate between random clusters of symptoms and an outbreak. It is the awareness that symptoms are connected in some way to consumption of or exposure to a particular source, or the association of patients within a social group or across separate geographical locations. Detection is the moment when physicians, epidemiologists, or public health officials “connect the dots,” making the distinction between normal day-to-day illness and a genuine outbreak or pandemic.

Attribution is a higher level of awareness. It occurs when the outbreak source has been identified, and when it is credited to a criminal act or terrorism. Attribution is, in particular, not only the acknowledgement of an outbreak but also the assessment that it is not resulting from natural causes. More than detection, attribution has a significant role to play in the future of U.S. national security strategy, as a desirable element is the ability to link attacks back to the actor. From a homeland defense and counterterrorism perspective, rapid and reliable BW attribution can appreciably improve U.S. strategic position by enabling WMD dissuasion and deterrence. If it can be known that the United States will neutralize and quickly recover from biological attacks, and then identify the responsible enemy, then would-be adversaries may be dissuaded from pursuing or attempting to acquire a biological capability. Likewise, those already having one may be deterred. Detection through surveillance and attribution through cooperation are the requirements drawn from the lessons learned in the 1984 Rajneesh and 2001 anthrax case studies.

A. CASE COMPARISON

The covert 1984 attack resulted in many victims, while the overt 2001 attack resulted in few casualties. The first used a moderate-grade Category B agent, while the second used a highly sophisticated strain of a lethal Category A agent. The

²⁴² National Defense University, *Toward a National Biodefense Strategy*, 32.

covert/moderate attack was slow to be detected and almost escaped attribution, while the overt/lethal attack was more quickly detected and almost immediately attributed to terrorism. While the perpetrators of the covert salmonella attack were eventually caught and imprisoned, the terrorist(s) in the overt anthrax attack remain free.

Therefore, the Rajneesh and anthrax attacks differ in nature of attack (overt versus covert), the lethality of agent used (Category A, B, C), the surveillance and epidemiological investigation of events, and the detection and eventual attribution of the attacks. Understanding the relationship between these elements is important, because it shows areas that can be improved to increase national preparedness for future biological attacks. The two core areas for improvement as revealed by the case studies are in surveillance and interagency cooperation between public health and law enforcement.

Speed of detection depends on successful medical surveillance. While this seems obvious for concealed attacks such as that conducted by the Rajneeshees, it also proved true for the explicit anthrax attacks, as victims were misdiagnosed and sent home after initially reporting to the hospital with inhalation symptoms.²⁴³ Positive attribution depends on cooperation between public health and law enforcement. While this seems obvious from the flawed epidemiological reports and belated criminal investigation in the Rajneeshee case, it also proved true in the aftermath of 9/11 and the more obvious anthrax attacks. Despite heightened national concerns, the threatening letters, and the very presence of anthrax, government officials from the Department of Justice, FBI, HHS, and CDC were initially unconvinced and required each other's expertise to determine if a bioterrorism event had occurred. Debate over the characteristics of the agent used and its connection to either a state or non-state actor underscores this fact.

Comparing the Rajneesh and anthrax cases shows that both nature of attack and agent type play a role in the speed of detecting outbreaks, as well as whether they are likely to be attributed to natural causes versus a criminal act. From this it is further shown that surveillance facilitates detection, while cooperation facilitates attribution. If these hold to be true, then the implications are: 1) that covert/moderate attacks should be

²⁴³ John A. Jernigan et al., "Bioterrorism-related Inhalational Anthrax: The First 10 Cases Reported in the United States," *Journal for Emerging Infectious Diseases* 7, no. 6 (November-December 2001), 937, <http://www.cdc.gov/ncidod/EID/vol7no6/pdf/jernigan.pdf> (accessed December 3, 2005).

the more attractive option for bioterrorists if their objective is not mass destruction, 2) that such attacks present the greatest challenge for the United States in the future, and 3) that improving detection through surveillance and attribution through cooperation is vital to mitigate possible future threats. These implications are examined further in Chapter V when considering the future framework of bioterrorism.

B. NOTIONAL MODEL OF BIODEFENSE

The implications, then, are that robust detection and attribution capabilities are important not only to discern covert/moderate attacks, but are also vital in managing the most obvious and deadly attacks as well. When attacks are overt, such as the anthrax letters (presence of agent is announced or credit is taken immediately or shortly after the attack), one would expect detection to happen rather quickly. In cases like this, first-tier attribution occurs when the substance is identified and law enforcement confirms that terrorist claims are not a hoax (second-tier being actual identification of the perpetrator). Cooperation is still required for attribution, even during overt attacks. This is because law enforcement must work with patients, physicians, and public health officials in the conduct of criminal investigations, and must also work with scientists to determine the validity of evidence.

Agent type or lethality can also determine both the speed of detection and likelihood of attribution. Common and naturally occurring pathogens and the infections they create raise little medical suspicion and are not assumed to be the weapon of choice for terrorists. With regard to detecting an outbreak, salmonella did not raise the same level of suspicion as did inhalational anthrax. The rarity of naturally occurring anthrax made it more easily attributed to terrorism, whereas the salmonella outbreak was thought to be an accident for more than a year. Thus, the type of agent used influences the speed of detection and chances of attribution.

Therefore, both the nature of attack and agent type impact detection of infectious disease outbreaks, however they are caused. The implications are that future attacks may be overt, covert, deadly, or benign, and that national biodefense preparedness relies on effective medical and public health surveillance to detect the full spectrum of possible threats.

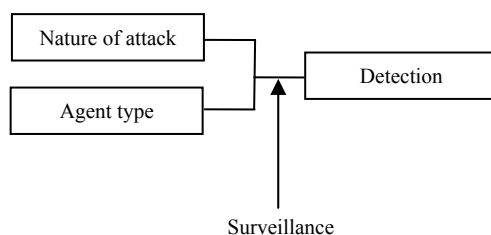


Figure 5. Surveillance facilitates detection.

Furthermore, nature of attack and agent type also affect the ability to attribute outbreaks to an actual attack. The implication again is that future attacks may run the gamut of overt, covert, deadly, or benign, and the U.S. public health system and law enforcement agencies must cooperate for attribution to occur.

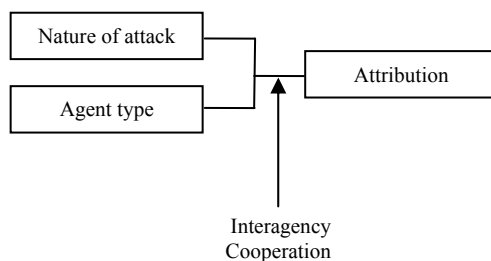


Figure 6. Interagency cooperation facilitates attribution.

In sum, medical surveillance facilitates detection (Figure 5), whereas interagency cooperation facilitates attribution (Figure 6). If this is the case, then current U.S. biodefense strategy should be examined in light of these findings.

C. BALANCING NATIONAL PRIORITIES

Today's biodefense dollars are being spent on programs that do not necessarily improve detection through better surveillance, or attribution through improved interagency cooperation. The bulk of funds are being spent to build new facilities and award government contracts to private companies for the development of next-generation vaccines to counter advanced biological agents. The National Biodefense Analysis and Countermeasures Center (NBACC) and numerous private sector contracts demonstrate

this point.²⁴⁴ This approach to improving U.S. biodefense preparedness has been so difficult that legislation was recently passed to create the Biomedical Advanced Research and Development Authority (BARDA) to oversee and award such contracts, with the intent to “facilitate collaboration and promote innovation.”²⁴⁵

Programs such as Projects BioShield, BioWatch, and BioSense do aim to improve national surveillance and response capabilities, but they will only be as successful as the stakeholders and collaborative networks that use these systems.²⁴⁶ No amount of pre-positioned vaccine from BioShield and the Strategic National Stockpile will help if state and local officials can not access, control, and distribute the medical countermeasures. BioWatch sensors are meaningless if those monitoring do not relay warnings to the

²⁴⁴ The NBACC is estimated to cost \$128 million and will be the first Department of Homeland Security laboratory specifically dedicated to biodefense. Examples of government awarded biodefense contracts include but are not limited to \$5.3 million to DOR Biopharma for development of advance ricin and botulinum toxin vaccine, \$24.7 million to Achaogen, Inc. for the development of therapies to combat anthrax and plague, and \$877.5 million to VaxGen, Inc. for development of a next-generation anthrax vaccine under Project BioShield. Dana A. Shea, *The National Biodefense Analysis and Countermeasures Center: Issues for Congress* (Washington, D.C.: Congressional Research Service, October 4, 2006), and Genetic Engineering News, “DOR Biopharma Awarded \$5.3M to Advance Ricin Toxin and Botulinum Toxin Vaccine Programs,” <http://www.genengnews.com/news/bnitem.aspx?name=6256619> (accessed November 8, 2006), and CNW TELBEC, “Achaogen Awarded \$24.7M Biodefense Contract by DTRA,” <http://www.cnw.ca/fr/releases/archive/October2006/24/c4159.html> (accessed November 8, 2006), and Paul Elias, “BioShield Dispute Underscores Problems with Defense Program,” *The Mercury News*, http://www.mercurynews.com/mld/mercurynews/news/breaking_news/15590348.htm (accessed November 8, 2006).

²⁴⁵ BARDA was part of H.R. 5533 passed September 27, 2006, as the *Biodefense and Pandemic Vaccine and Drug Development Act of 2006*. Biotechnology Industry Organization, “House Moves to Shore Up Nation’s Biodefenses by Passing BARDA Bill,” <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/09-28-2006/0004441946&EDATE=> (accessed November 8, 2006).

²⁴⁶ The *Project BioShield Act of 2003* represents a crash plan to acquire and stockpile next-generation vaccine and drugs by appropriating \$5.6 billion over ten years to purchase countermeasures against anthrax, smallpox, and other agents. BioWatch is an early warning system of sensors that can rapidly detect trace amounts of biological material in the air, whether from intentional release or from minute natural quantities existing in the environment. BioSense, a component of the existing Public Health Information Network, includes an internet-based software system that will enable public health officials in major cities to view data for their communities in near real-time. Department of Health and Human Services, “HHS Fact Sheet: Project BioShield,” <http://www.hhs.gov/news/press/2004pres/20040721b.html> (accessed December 16, 2005), and Department of Homeland Security, *BioWatch: Early Detection, Early Response* (Washington, D.C.: Science and Technology Directorate, n.d.), <http://www.milnet.com/wh/DoHS/BioWatchFactSheetFINAL.pdf> (accessed December 16, 2005), and Department of Health and Human Services, “PHIN: BioSense,” Centers for Disease Control and Prevention, <http://www.cdc.gov/phin/component-initiatives/biosense/> (accessed December 16, 2005), and John W. Loonsk, “BioSense—A National Initiative for Early Detection and Quantification of Public Health Emergencies,” *Morbidity and Mortality Weekly Report* 53, Supplement (September 24, 2004), 53, <http://www.cdc.gov/MMWR/preview/mmwrhtml/su5301a13.htm> (accessed December 16, 2005).

people who need them most.²⁴⁷ Finally, the BioSense national architecture will only be as good as those using the system. Medical officials, physicians, pharmacies, and many others must embrace and use the network. While these consequence management capabilities are important, it also follows that “extraordinary measures are not necessary to develop a comprehensive terrorism health surveillance and epidemiologic network.”²⁴⁸

According to the CDC, successful disease surveillance and epidemiological response requires collaboration among partners in Table 4 and the response of actors in Table 5 below.

State health departments Emergency medical services Social service agencies Hospitals Clinics and physicians Epidemiologists Medical examiners/coroners Laboratories	County health departments Dispatch/911 Volunteer organizations Mental health professionals Poison centers Pharmacists Veterinary services
---	---

Table 4. Surveillance partners. (From: *The Public Health Response*, July 2001, 14.)

Health Directors Governors Mayors Law enforcement agencies Local health departments Public Information Officers Department of Agriculture staff	Emergency Management Directors Fire/rescue/EMS Hazardous material teams Legal counsel Managed care representatives Environmental Protection Agency staff
---	---

Table 5. Response actors. (From: *The Public Health Response*, July 2001, 70.)

In addition, CDC planning guidance says that “well-developed surveillance and epidemiological capacity is the foundation on which health departments will detect,

²⁴⁷ Inconclusive tests prevented the Department of Homeland Security from notifying federal and local health agencies that sensors in the Washington, D.C. National Mall had detected tularemia. CDC did not learn of the biosensor readings for at least 72 hours, and it took five days for D.C.–area health agencies to receive the news. Global Security Newswire, “Inconclusive Test Results Cited in Delayed Tularemia Notification to Federal, Local Health Agencies,” http://www.nti.org/d_newswire/issues/2005/10/5/35653f39-93ee-416f-9540-a8cc79aaf652.html (accessed December 20, 2005).

²⁴⁸ Department of Health and Human Services, *The Public Health Response*, 15.

evaluate, and design effective responses to terrorism events.”²⁴⁹ Even so, studies repeatedly conclude that U.S. capacity for timely detection of outbreaks varies widely, and the most difficult ones are fraught with significant delays.²⁵⁰

Where documentation is available, outbreaks with a delay of 12 days or more from onset of illness to discovery are common.²⁵¹ Outbreak investigations conducted by the CDC’s EIS between 1988 and 1999 found that of 1,099 cases, public health departments, healthcare providers, and medical practitioners combined reported 66.8 percent of all cases.²⁵² Reporting was delayed for up to 26 days for six of these outbreaks where bioterrorism or intentional contamination was possible.²⁵³ More recently during the September 2006 U.S. *E. Coli* spinach outbreak, it took two months for an 80-year-old woman’s symptoms to be linked to the outbreak through official surveillance reporting methods.²⁵⁴ Finally, delays for emerging infections are even greater, with identification taking from weeks to years. The U.S. capacity for timely detection of disease outbreaks varies so widely because there are more than 66 national disease detection systems spread among all levels of government and between public and private entities.²⁵⁵ Detection results from “the concatenated, cooperative effort of local, state, and federal entities. This capacity is not tightly coordinated, not well described, and is ever changing...”²⁵⁶

²⁴⁹ Department of Health and Human Services, *The Public Health Response*, 11.

²⁵⁰ Michael M. Wagner et al., *The Nation's Current Capacity for the Early Detection of Public Health Threats Including Bioterrorism* (Rockville, MD: Agency for Healthcare Research and Quality, September 26, 2001), v, <http://rods.health.pitt.edu/LIBRARY/dato1AHRQInterimRpt112601.pdf> (accessed March 29, 2006).

²⁵¹ Ibid.

²⁵² David A. Ashford et al., “Planning against Biological Terrorism: Lessons from Outbreak Investigations,” *Emerging Infectious Disease* 9, no. 5 (May 2003): 515.

²⁵³ Ibid.

²⁵⁴ Author interview with Cindy Lambdin of U.C. Berkeley’s School of Public Health, Center for Infectious Disease Preparedness on November 15, 2006. Interview conducted during California’s annual *Golden Guardian* disaster preparedness exercise. Also see Centers for Disease Control and Prevention, “Multiple States Investigating a Large Outbreak of *E. Coli* O157:H7 Infections,” Health Alert Network, <http://www2a.cdc.gov/HAN/ArchiveSys/ViewMsgV.asp?AlertNum=00249> (accessed November 16, 2006).

²⁵⁵ Wagner et al., *The Nation's Current Capacity*, Appendix III Detection Systems, 66-77.

²⁵⁶ Ibid., v.

Taken together the delays in detection...make it clear that the National Detection System cannot detect outbreaks of disease with the timeliness needed for an optimal response to many bioterrorist releases, which are by intention selected for maximal speed and impact. Poor sensitivity is an issue for the detection of smaller or dispersed bioterrorist releases, or for detection of premonitory releases.²⁵⁷

Sometimes the simpler and less costly fixes are overlooked. Today there is a need to re-balance national biodefense priorities—to ease emphasis on current infrastructure programs, and to redirect valuable resources towards rudimentary improvements in communication and organizational efficiency. The next two sections consider today's top three public health limitations and the power of collaborative networks to enhance detection through surveillance and attribution through coordination.

D. DETECTION: SURVEILLANCE AND PUBLIC HEALTH LIMITATIONS

This section begins by defining detection, epidemiology, and surveillance in terms of public health. This is important for understanding the organization and limitations of the U.S. public health system which are presented next. The section concludes by presenting the National Biosurveillance Integration System (NBIS) as a surveillance system which holds promise. While an achievement, NBIS is incomplete without enhancing interagency coordination for BW attribution.

1. Detection, Epidemiology, and Surveillance Defined in Terms of Public Health

Detection is the act of determining the existence, presence, or characteristics of outbreaks that permit response.²⁵⁸ The goals of detection are two-fold. First is to discover the existence of some anomaly, such as an unusual cluster of deaths in people who attended a public gathering, and then to verify that it is an outbreak. Second is to characterize the anomaly by isolating the specific agent and identifying the common source. Elements of characterization include determining the presumed route of transmission, incubation periods, and host characteristics such as age or coexisting illnesses.²⁵⁹ As a subfield of medicine, epidemiology helps characterize anomalies as it is concerned with “the study of patterns of disease occurrence in human populations or,

²⁵⁷ Wagner et al., *The Nation's Current Capacity*, vi.

²⁵⁸ *Ibid.*, 3.

²⁵⁹ *Ibid.*, 4.

even more broadly, the comparison of rates of occurrence of phenomena in various populations.”²⁶⁰ A list of epidemiological clues that may signal a covert BW attack are provided below.

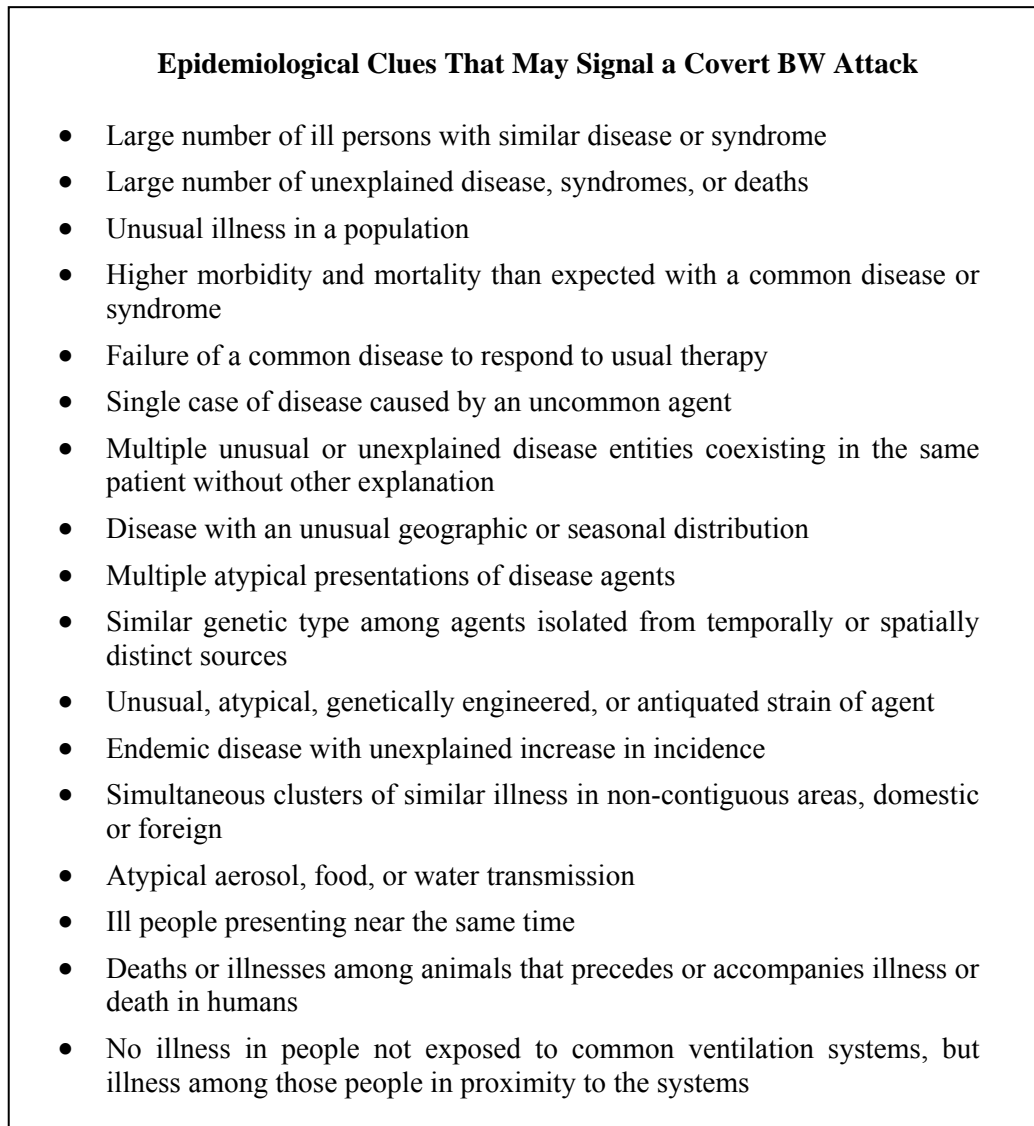


Figure 7. Epidemiological Clues That May Signal a Covert BW Attack. (From: *The Public Health Response*, Exhibit 2, 17.)

Public health surveillance enables detection, and includes “the routine collection, analysis and dissemination of all data that may be relevant for the prevention and control

²⁶⁰ David W. Fraser, “Epidemiology as a Liberal Art,” *The New England Journal of Medicine* 316, no. 6 (February 5, 1987): 310.

of a public health problem.”²⁶¹ Two broad goals of surveillance relating to bioterrorism preparedness are early detection and enhanced disease tracking during emergency response.²⁶² In order to be effective, “surveillance data must be linked to the appropriate authorities who will investigate unusual instances...and clusters of illness or death,” and must also be linked to emergency response officials at local and state levels.²⁶³

In the field of public health surveillance there are two methods of data collection: active and passive.²⁶⁴ In active surveillance people proactively gather data. An example of active surveillance is the United States Influenza Sentinel Physicians Surveillance Network, in which select medical practices agree to collect and report information related to influenza on a weekly basis. Passive surveillance is reactive, and relies on a system whereby information is gathered and delivered after events unfold. An example of passive surveillance is the reporting of disease in which clinicians, medical practices, and laboratories are required to report cases. The advantage of active over passive surveillance is more complete (and potentially timely) data collection. The disadvantage is cost, which can limit the application of active systems to improve overall “timeliness and completeness of detection.”²⁶⁵

It is with knowledge of these terms as they relate to public health (detection, epidemiology, and the methods of surveillance) that the composition and limits of the U.S. public health system can best be understood.

2. Composition and limits of the U.S. Public Health System

The U.S. public health infrastructure works to “decrease the burden of illness and injury in populations, rather than individuals.”²⁶⁶ It uses epidemiological investigation, laboratory testing, information technology systems, and public and provider education

²⁶¹ Wagner et al., *The Nation's Current Capacity*, 3.

²⁶² Department of Health and Human Services, *The Public Health Response*, 45.

²⁶³ *Ibid.*, 45-6.

²⁶⁴ Wagner et al., *The Nation's Current Capacity*, 4.

²⁶⁵ *Ibid.*, 4-5.

²⁶⁶ Lister, *An Overview of the U.S. Public Health System*, i.

schemes to accomplish its mission, and it relies heavily on an adequate and well-trained workforce for success.²⁶⁷ In the United States, this system is comprised of “a wide array of governmental and nongovernmental entities,” to include:

- over 3,000 county and city health departments and local boards of health;
- 59 state and territorial health departments;
- tribal health departments;
- more than 160,000 public and private laboratories;
- parts of multiple federal departments and agencies;
- hospitals and other healthcare providers; and
- volunteer organizations such as the Red Cross.²⁶⁸

These form the federal, state, tribal, and local resources available to accomplish the mission, and they interact with a broad range of other partners to ensure public health.²⁶⁹

In the context of preparedness, the key functions of the U.S. public health system include:

...disease surveillance to detect outbreaks and to monitor trends; specialized laboratory testing to identify bioagents, ...epidemiologic methods to identify persons at risk and to monitor the effectiveness of prevention and treatment measures; knowledge of disease processes in populations to determine appropriate responses such as quarantine, decontamination or the dissemination of treatment recommendations; and coordination with partners to establish effective planning and response.²⁷⁰

To accomplish these key functions, the system relies on several independent components that span all levels of government, as well as the public and private sector. These components are embodied in 1) the public health workforce, 2) the healthcare sector, 3) laboratories, and 4) information technology infrastructure.²⁷¹ The implications for bioterrorism preparedness are that a deficiency or failure in any of these components can

²⁶⁷ Lister, *An Overview of the U.S. Public Health System*, i.

²⁶⁸ Ibid., CRS-3.

²⁶⁹ Ibid.

²⁷⁰ Ibid., CRS-3-4.

²⁷¹ The public health workforce includes government employees who interact with individuals in the public and private healthcare sector, in academia, and in volunteer organizations. The healthcare sector includes “hospitals, clinics, pharmacies, emergency medical services, [and] a host of ancillary services...” Ibid., CRS-4.

lead to unsuccessful surveillance and detection of BW attacks. Additionally, the compounded problem of incubation periods and time delays between attack and symptom onset present decision problems for public health workers that can prevent a timely transition to response.

Public health responses can range from the collection of more information to actual dispatch of treatment task forces.²⁷² “Responses have different costs and different expected benefits and can be initiated at any time. Thus, public health officials face a continuous decision problem of whether to initiate one or more potential responses.”²⁷³

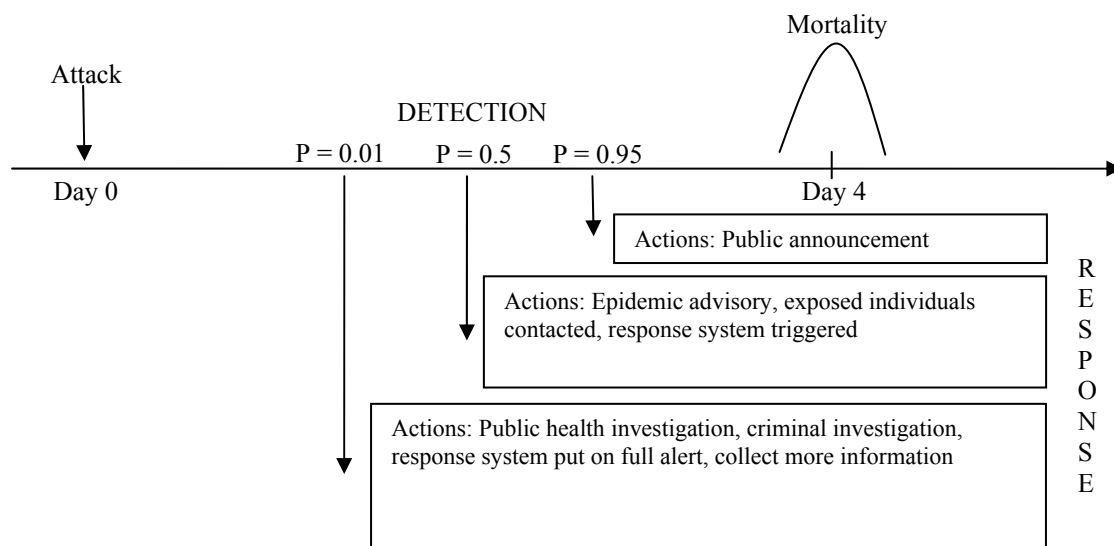


Figure 8. The Connection between Detection and Response. (From: Wagner et al., *The Nation's Current Capacity*, 6.)

The time problem illustrated in Figure 8 above, combined with the fact that the U.S. public health system relies most heavily on reactive passive surveillance, results in three key limitations. These limitations are in the form of organizational structure, laboratory capacity, and the National Detection System.

a. Limitation: Organizational Structure

U.S. disease surveillance capabilities result from “the often voluntary cooperation of many public health entities utilizing many information systems.”²⁷⁴ The

²⁷² Wagner et al., *The Nation's Current Capacity*, 4.

²⁷³ Ibid.

²⁷⁴ Ibid., 23.

surveillance architecture is so complex because it contains numerous interrelated subsystems operated by vastly different entities to include public and private sector, local, state, and federal agencies.²⁷⁵

There is significant state-to-state variability in the existing public health system, and also variability at the local levels. Effectively, each of the 50 states has its own detection systems since public health surveillance at the state and local level is based upon the constitutions, regulations, rules, and common law of each state. Some states...have state control of the local health districts, some...have home rule with many local health departments and some...have a mix of local health departments and regional health districts.²⁷⁶

This variance affects jurisdiction and whether local or state officials will initially perform the functions of triage, contact tracing, and case or outbreak investigations. Some uniformity across states does result from voluntary coordination through the Council of State and Territorial Epidemiologists regarding sets of reportable diseases. Another voluntary network is the Infections Disease Society of America, which sends aggregate reports of illness to the CDC. However, these are voluntary, and represent only two of 66 identified surveillance systems in the United States.²⁷⁷

Detection can first occur in reference laboratories sometimes located at universities or federal institutions. “The aggregation of a number of...requests [for tests] from different hospitals can be an important tip-off of an outbreak.”²⁷⁸ Regarding the national capacity to detect outbreaks, a failure at any level in the system can and will delay or entirely eliminate the chance of detection, especially for small outbreaks. Success requires “cooperation and funding by local, state, federal, and private organizations, all working under a variety of rules and constraints.”²⁷⁹ Two problems arise as a result. First is the problem of heavy reliance on clinical diagnosis and test results before public health officials can act. When early warning is critical, such as in bioterrorism, “the current system, even under optimal conditions, would operate with so

²⁷⁵ Wagner et al., *The Nation's Current Capacity*, 24.

²⁷⁶ *Ibid.*, 26.

²⁷⁷ *Ibid.*, 24.

²⁷⁸ *Ibid.*, 26.

²⁷⁹ *Ibid.*, 27.

many built-in delays that opportunities for prophylaxis would be lost.”²⁸⁰ Second is the problem of heavy reliance on multiple local jurisdictions to assess outbreaks. This leads to a potential lack of sensitivity in surveillance. No one jurisdiction may have enough medical cases to recognize that an anomaly exists.²⁸¹

The public health system faces various barriers to achieving successful surveillance and detection of surreptitious BW attacks. In 1999, the Institute of Medicine said that real-time detection of biological agents in the environment is problematic, “because of the number of potential agents to be distinguished, the complex nature of the agents themselves, the myriad of similar microorganisms that are always present in the environment and the impracticality of providing real-time, continuous monitoring.”²⁸² Since the Rajneesh attacks in 1984, and especially since the anthrax attacks of 2001, improvements in the U.S. laboratory system and the National Detection System represent two approaches taken to fix these problems. Unfortunately, limitations remain in these two areas.

b. *Limitation: Laboratory Capacity*

The U.S. laboratory system and its capacity for detecting the presence of biological agents reside at four levels.²⁸³ Level A laboratories are public health department and hospital labs with a certified biological safety cabinet as a minimum. Level B (core capacity) laboratories are state and local health department labs with Biosafety Level (BSL) 2 facilities that incorporate BSL-3 procedures and maintain proficiency to “adequately process environmental samples, rule in specific agents, and perform confirmatory and antibiotic susceptibility testing.”²⁸⁴ These laboratories can contact higher-level labs and forward samples for further study. Level C (advanced capacity) laboratories are BSL-3 facilities with the ability to “perform nucleic acid amplification, molecular typing, and toxicity testing.”²⁸⁵ These laboratories can perform the duties of Level B labs, as well as provide limited surge capacity when needed.

²⁸⁰ Wagner et al., *The Nation's Current Capacity*, 27.

²⁸¹ Ibid.

²⁸² Quoted in Wagner et al., *The Nation's Current Capacity*, 2.

²⁸³ Department of Health and Human Services, *The Public Health Response*, 46.

²⁸⁴ Ibid.

²⁸⁵ Ibid., 47.

Finally, Level D laboratories “can validate new assays, detect genetic recombinants, provide specialized reagents, securely bank isolates, and possess BSL-3 and BSL-4 biocontainment facilities.”²⁸⁶ The CDC has a Level D laboratory for bioterrorism events that affect civilian populations.

The Laboratory Response Network (LRN) is an association of federal, state, and local laboratories that provide coordinated sample collection, transport, testing, surge capacity, and training to identify key biological and chemical agents.²⁸⁷ The system represents a pyramid of sentinel, reference, and national laboratories.²⁸⁸ Sentinel laboratories serve hospitals, clinics, and other first-points-of-contact for victims, and are not equipped to handle pathogens likely to be used in BW attacks. For this reason they only perform “recognize/rule out/refer” services.²⁸⁹ Protocol requires the system of over 25,000 sentinel labs to contact state reference labs when suspecting the presence of BW agents.²⁹⁰ Reference facilities comprise more than 100 state and local public health, military, international, veterinary, agriculture, food, and water testing laboratories.²⁹¹ They provide investigation and/or referral of specimens through confirmation testing. Definitive characterization of BW agents through microbial forensic analysis is done in national BSL-4 facilities at CDC and USAMRIID.

The Rajneesh attacks overwhelmed state and local laboratories in Oregon. Moreover, the anthrax attacks “challenged the network’s resources and exposed a gap in planning for communication of results.”²⁹² Between October and December 2001, the LRN processed over 125,000 samples of anthrax directly relating to exposures in seven states and the District of Columbia, as well as threat samples from all remaining states.²⁹³ As a result, current LRN initiatives include funding to acquire BSL-3 capability in all

²⁸⁶ Department of Health and Human Services, *The Public Health Response*, 47.

²⁸⁷ Lister, *An Overview of the U.S. Public Health System*, CRS-35.

²⁸⁸ Centers for Disease Control and Prevention, “Laboratory Network for Biological Terrorism,” <http://www.bt.cdc.gov/lrn/biological.asp> (accessed December 19, 2005).

²⁸⁹ *Ibid.* and Lister, *An Overview of the U.S. Public Health System*, CRS-35.

²⁹⁰ Centers for Disease Control and Prevention, *Laboratory Network for Biological Terrorism*.

²⁹¹ *Ibid.*

²⁹² Lister, *An Overview of the U.S. Public Health System*, CRS-35.

²⁹³ *Ibid.*

states, preparing a timeline for providing at least one epidemiologist for each metropolitan area with a population greater than 500,000, and conducting at least one exercise annually to test laboratory readiness.²⁹⁴

c. *Limitation: The National Detection System*

The Nation's Current Capacity for the Early Detection of Public Health Threats Including Bioterrorism remains the best source available on America's ability to detect disease. The research team's goal was to analyze U.S. capacity to detect major biological threats, "both natural and terrorist in origin, new, old and future, as a necessary first step to recommending improvements..."²⁹⁵ Because the scope could be quite large, research was limited to only significant public health threats to humans occurring solely in the United States. Despite this, the team identified 66 separate detection systems which it called the National Detection System, illustrated in Figure 9 on the following page. The graphic is confusing because it represents the voluntary cooperation of numerous public health entities, using various information systems, across all levels of government. The surveillance architecture is complex because of interrelated subsystems operated by vastly different stakeholders which include public and private sector, local, state, and federal agencies.²⁹⁶ While an argument can be made that such a surveillance framework increases redundancy and the overall chances of detection, the team of experts concluded otherwise:

Taken together the delays in detection, and to a lesser extent the speed at which characterization proceeds, make it clear that the National Detection System cannot detect outbreaks of disease with the timeliness needed for an optimal response to many bioterrorist releases, which are by intention selected for maximal speed and impact.²⁹⁷

²⁹⁴ Lister, *An Overview of the U.S. Public Health System*, CRS-36, 49-50.

²⁹⁵ Wagner et al., *The Nation's Current Capacity*, iv.

²⁹⁶ *Ibid.*, 24.

²⁹⁷ *Ibid.*, vi.

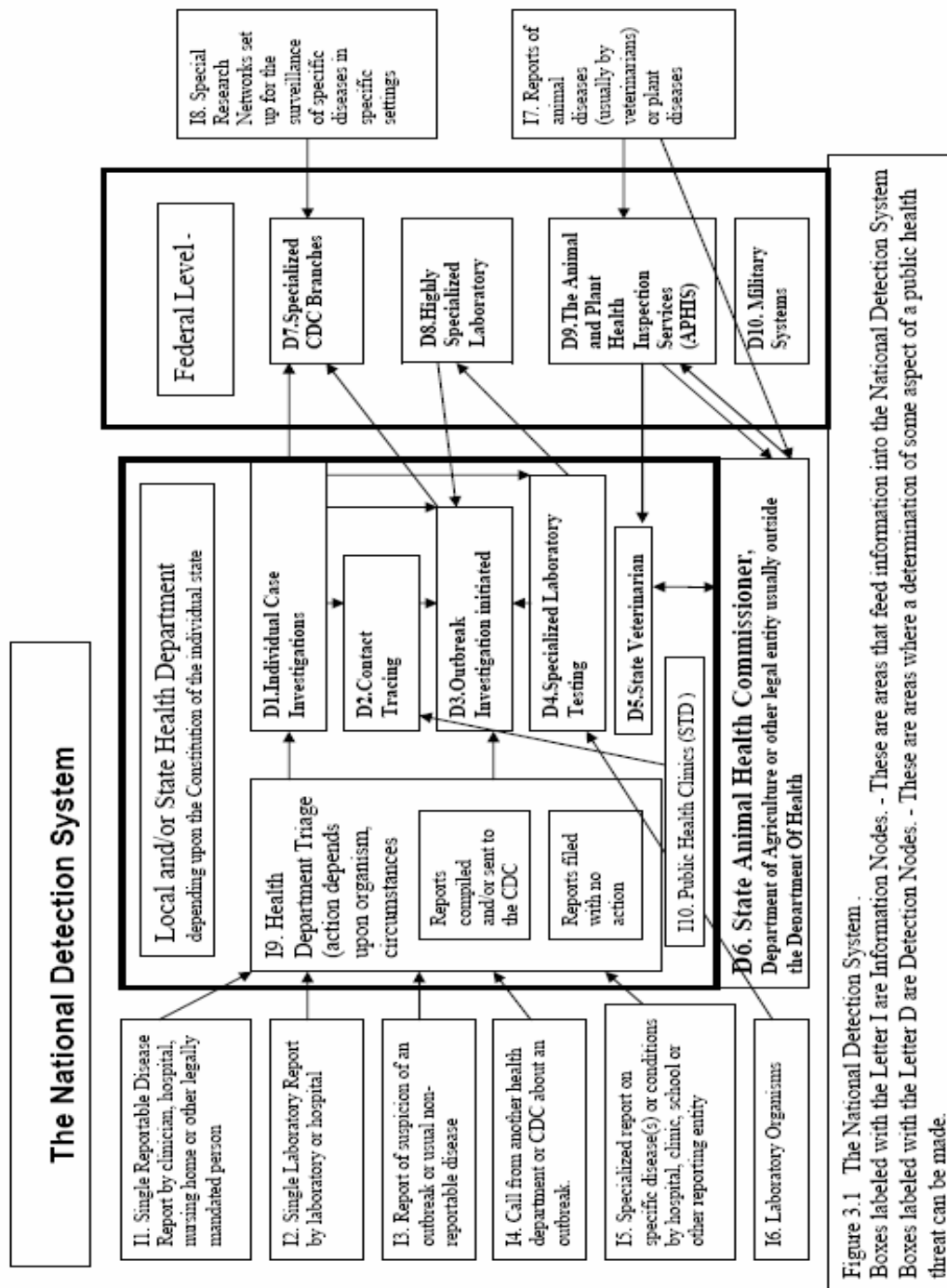


Figure 3.1 The National Detection System .
Boxes labeled with the Letter I are Information Nodes. - These are areas that feed information into the National Detection System
Boxes labeled with the Letter D are Detection Nodes. - These are areas where a determination of some aspect of a public health threat can be made.

Figure 9. The National Detection System (From: Wagner et al., *The Nation's Current Capacity*, Figure 3.1, 25.)

If active surveillance is too expensive, and passive surveillance suffers from under-reporting, then what options are available to improve the National Detection System? The report used signal detection and decision theories to recommend four possible avenues of improvement. These were to improve the quality of existing signals, to add new signals, to improve the algorithm for processing signals, or to optimize the detection threshold.²⁹⁸ Of these, the area that is most practical and is being pursued today by the U.S. Department of Homeland Security (DHS) is in the area of adding signals.

Signals can be added through both passive and active means. Passive surveillance can be enhanced by removing barriers while at the same time adding incentives that encourage reporting. Systems that persuade direct physician early reporting are most beneficial. Barriers can be removed by making forms available on the Internet, and incentives can be provided by giving physicians information about similar cases.²⁹⁹ The high costs associated with active surveillance can be reduced by leveraging data already collected routinely for other purposes. This minimizes the cost to develop and maintain special purpose data collection systems. Furthermore, “value-of-information consideration” is a decision theory principle that can reduce costs further by calculating the utility of whether to collect certain kinds of information.³⁰⁰ These principles find direct application in today’s National Biosurveillance Integration System.

3. The National Biosurveillance Integration System (NBIS)

NBIS is a government-wide system managed by DHS. It is intended to “combine multiple data streams from sector-specific agencies—those with health, environmental, agricultural, and intelligence data—to provide all stakeholders with broad situational awareness that is expected to allow for earlier detection of events and to facilitate coordinated response.”³⁰¹ The goal is to “collect, assemble, and analyze a wide range of relevant information and make such information available to government stakeholders in

²⁹⁸ Wagner et al., *The Nation's Current Capacity*, 49-51.

²⁹⁹ Ibid., 50.

³⁰⁰ Ibid.

³⁰¹ Gary Cecchine and Melinda Moore, *Infectious Disease and National Security* (Santa Monica, CA: RAND National Defense Research Institute, 2006), 24.

a timely and reliable fashion.”³⁰² When operational, NBIS will consolidate information in a common platform, and will coalesce this information with environmental and intelligence data. The new surveillance system will be used by DHS analysts to provide a common picture for public health surveillance to DHS’s Homeland Security Operations Center, and the Interagency Incident Management Group as described in the National Response Plan.³⁰³

NBIS was originally intended for bioterrorism, but its officials acknowledge that because it is difficult to discern between natural and deliberate outbreaks, it will also be useful in providing early warning of naturally occurring outbreaks.³⁰⁴ A central feature is software that actively probes or uses data-mining techniques to examine existing information sources. NBIS scans the Internet for reports (and even rumors of events) to systematically analyze over 1 million sites each day. “There is some evidence that this software has identified recent outbreaks significantly earlier than other systems have.”³⁰⁵

NBIS went from the requirements determination phase to the implementation phase in December 2004. While still under development, it aims to be “the ‘eyes and ears’ of the nation for indicators and warnings that prompt early detection of a disease outbreak, whether natural or deliberate in origin...”³⁰⁶ However, “it is not designed to replace existing agencies’ responsibilities for response, risk assessment, or forensic attribution.”³⁰⁷ Therefore, even though NBIS appears to be a move in the right direction to improve detection through better surveillance, it still does not replace the need for interagency cooperation and collaborative networks to realize rapid and reliable attribution.

³⁰² Cecchine and Moore, *Infectious Disease*, 24.

³⁰³ Ibid., 25. Also see Department of Homeland Security, *National Response Plan* (Washington, D.C.: Department of Homeland Security, May 25, 2006), http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml (accessed November 11, 2006) for information regarding the Interagency Incident Management Group and the National Response Plan.

³⁰⁴ Cecchine and Moore, *Infectious Disease*, 25.

³⁰⁵ Ibid.

³⁰⁶ Ibid.

³⁰⁷ Ibid.

E. ATTRIBUTION: COOPERATION AND COLLABORATIVE NETWORKS

Attribution requires cooperation between the private sector, academia, scientists, epidemiologists, physicians, public health officials, and law enforcement agencies.³⁰⁸ Thesis research, the case studies, and personal exercise participation have all shown that the relationship between public health and law enforcement is most vital for achieving BW attribution. This section begins by looking at how these two communities manage nature of attack and what specific roles they play in the surveillance and epidemiological process. It will be shown how subtle yet important differences between these two fields can hamper attribution. The section concludes by considering the emerging field of forensic epidemiology and revealing existing barriers to interagency coordination.

1. Managing Nature of Attack

Both law enforcement and public health officials emphasize the significance of attack nature in detecting and attributing bioterrorism. In testimony before Congress, Special Agent in Charge Larry Mefford of the FBI's San Francisco Division explained federal law enforcement's distinction between overt and covert BW attacks. If covert, the response is driven by the public health community. Initially there is no crime scene to investigate, and the criminal act may not be revealed until several days have elapsed.³⁰⁹ Once there is indication of a criminal act using a biological agent, the FBI assumes primary authority in conducting the criminal investigation while public health agencies retain responsibility for the welfare of citizens.

Covert attacks create coordination problems at the critical point shown in Figure 10 on the following page.

³⁰⁸ Anne L. Clunan, "Building Trusted Networks for Attributing Use of Biological Agents," paper presented at the Conference on Identification, Characterization, and Attribution of Biological Weapons Use, Center for Contemporary Conflict, U.S. Naval Postgraduate School and Kings College London, London, U.K., July 12-13, 2006.

³⁰⁹ House Committee on Government, *Terrorism Preparedness*, <http://www.fbi.gov/congress/congress02/mefford040202.htm> (accessed February 28, 2006).

Covert BW Attack Coordination

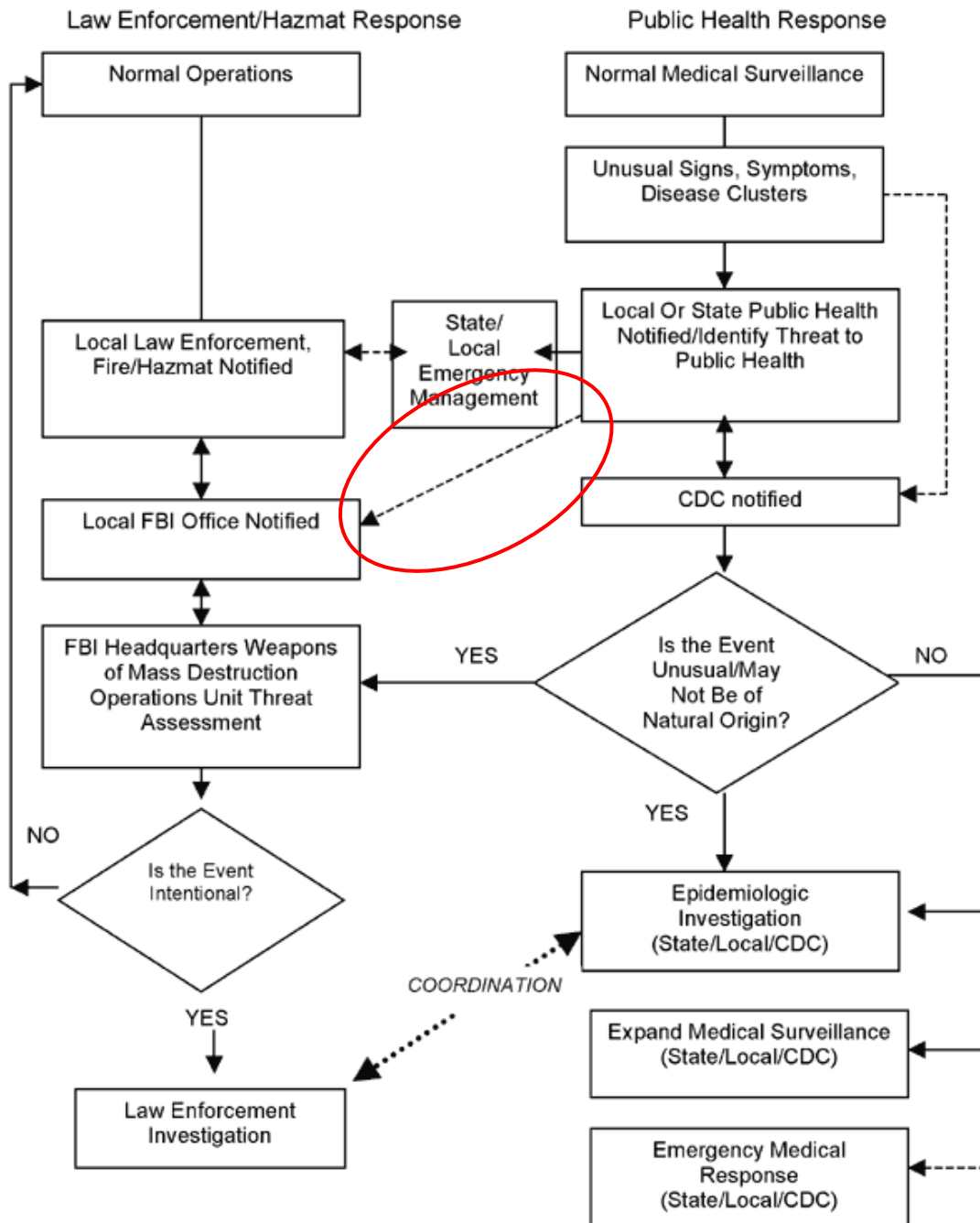


Figure 10. Law Enforcement and Public Health Coordination by Nature of Event – **Covert** BW Attack. (From: *Collaboration between Public Health and Law Enforcement*.)

Overt BW Attack Coordination

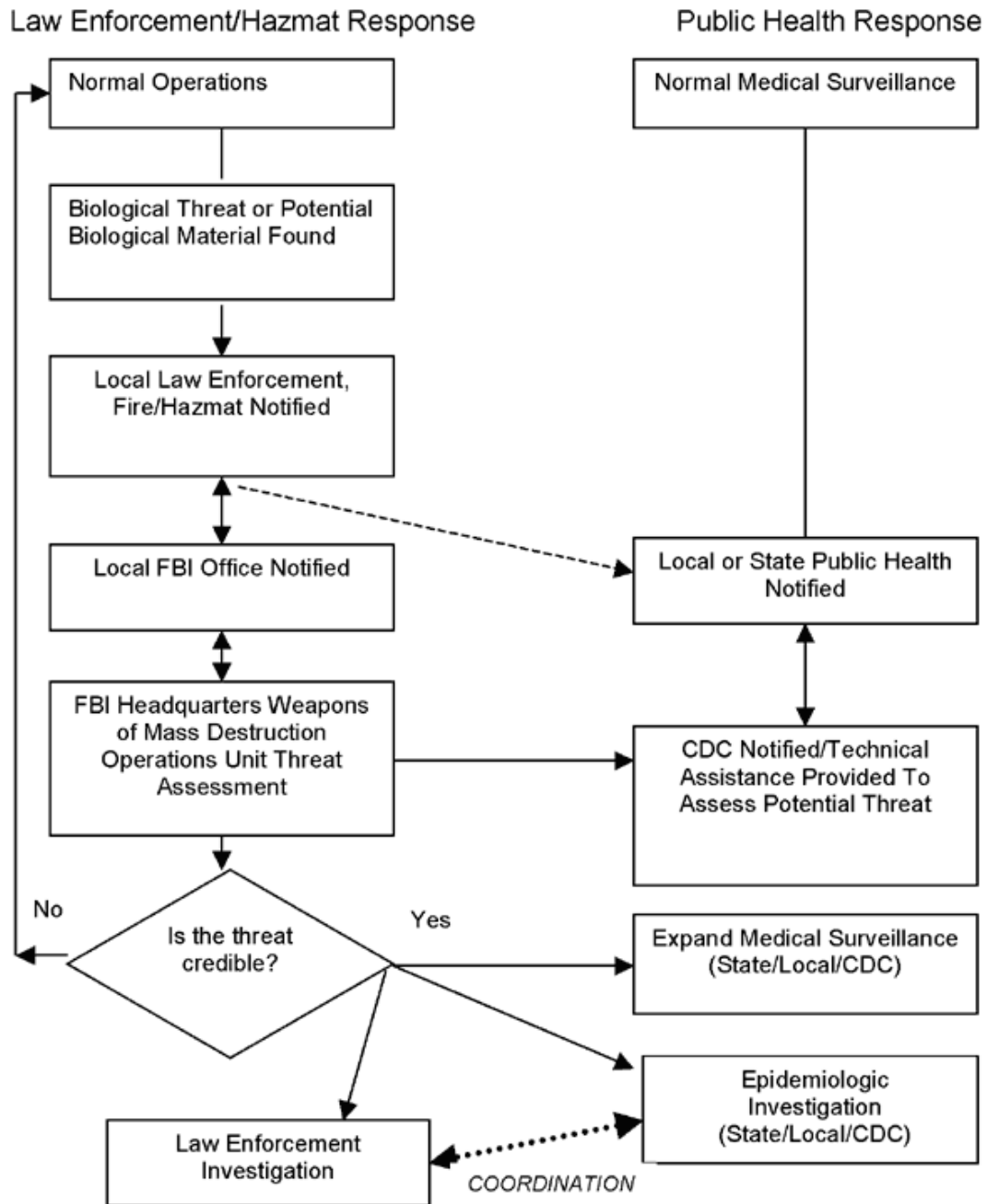


Figure 11. Law Enforcement and Public Health Coordination by Nature of Event – **Overt** BW Attack. (From: *Collaboration between Public Health and Law Enforcement.*)

If state or local health officials do not identify a threat (detection), and then do not contact law enforcement officials, outbreaks run the risk of never being attributed to terrorism. Such was the case with the Rajneesh cult, where the covert attacks were not attributed for more than a year. Operational and table-top exercises show time and again that state and local public health departments are reluctant to contact federal or local law enforcement.³¹⁰ This is because false calls can be embarrassing, and often there are delays for more tests and irrefutable medical evidence before contacting law enforcement.

The position of medical examiner highlights typical coordination challenges.³¹¹ Once under medical auspices to promote better understanding of death and disease, today medical examiners fall under the Sheriff's Department for evidentiary reasons and to support criminal proceedings. This line of authority (and associated loyalties) can vary from state to state. The evolution of this position moving from the public health arena to law enforcement has mainly been the result of funding issues over time—as hospitals have cut back to improve profit margins and as law enforcement has found more utility in the position of medical examiner.³¹² Unfortunately, the delays associated with public health's reluctance to contact law enforcement and the political loyalties of medical examiners can be deadly, as it takes three to five days before acute symptoms of inhalational anthrax appear.³¹³ While some deaths did occur in the Amerithrax case, the overt nature of the letters helped to transcend organizational barriers and facilitate quicker detection and attribution.

The CDC *Emerging Infectious Disease* article, "Collaboration between Public Health and Law Enforcement: New Paradigms and Partnerships for Bioterrorism Planning and Response," stresses why interagency cooperation is so important for successful detection and attribution of BW attacks. Collaboration between the CDC and

³¹⁰ Based on author participation in Monterey Institute of International Studies Workshop 548, "Simulating a Deliberately Caused Foodborne Disease Outbreak Using the Table-top Exercise (TTX)," Monterey, CA, November 4 and 12, 2005.

³¹¹ Author interview with Professor Craig Hooper, Scientist-in-Residence, Center for Nonproliferation Studies, Monterey Institute of International Studies, November 9, 2006.

³¹² Ibid.

³¹³ Carus, *Bioterrorism and Biocrimes*, 13.

FBI during the 2001 anthrax attacks highlighted the challenges to public health and law enforcement coordination in general. “Public health and law enforcement agencies become involved in the investigation of a possible bioterrorism event under different circumstances. Such events fall into one of two categories: overt and covert.”³¹⁴ The two possible sequence of events are shown in Figures 10 and 11 on pages 84 and 85. Before 2001, the collaborative efforts of CDC and FBI in establishing the LRN facilitated the coordination shown at the bottom of Figure 10. The need for validating tests that would be consistent with evidentiary requirements resulted in a uniform set of laboratory protocols based on established procedures.³¹⁵ This permitted the introduction of test results into a court of law, thereby reducing legal challenges and increasing the chances of conviction.³¹⁶ “The 2001 anthrax incidents demonstrated the importance of the LRN in responding to a biological attack and revealed the need to expand its laboratory capacities,” so that public health and law enforcement officials can better work towards detection and attribution.³¹⁷

2. Roles in the Surveillance and Epidemiological Process

The different and sometimes diametrically opposed goals of public health and law enforcement officials makes cooperation between the two difficult, as was revealed in both the Rajneesh and anthrax cases. The University of California Los Angeles Department of Epidemiology, School of Public Health, provides an excellent description of epidemiology and its distinction from law enforcement. It says epidemiologists are “disease detectives” that use similar methods as regular detectives in determining the cause of disease outbreaks, epidemics (a larger excess of disease), or pandemics (a worldwide excess of disease).³¹⁸ While the 2001 anthrax attacks share many of the same characteristics as typical outbreaks, the difference was that “there was no transmission

³¹⁴ Jay Butler et al., “Collaboration between Public Health and Law Enforcement: New Paradigms and Partnerships for Bioterrorism Planning and Response,” *Emerging Infectious Diseases* 8, no. 10 (October 2002), <http://www.cdc.gov/ncidod/EID/vol8no10/02-0400.htm> (accessed February 28, 2006).

³¹⁵ Ibid.

³¹⁶ Ibid.

³¹⁷ Ibid.

³¹⁸ UCLA Department of Epidemiology, School of Public Health, “American Anthrax Outbreak of 2001,” http://www.ph.ucla.edu/epi/bioter/detect/antdetect_intro.html (accessed March 1, 2006).

from infected to susceptible persons that linked one case to another.”³¹⁹ Nonetheless, deliberately infecting others with a deadly disease is a crime handled by police. Because the anthrax attacks involved more than one state and the USPS, the FBI was assigned jurisdictional control. Yet harm to victims was caused by *Bacillus anthracis*, calling for experienced disease rather than police detectives. This role was filled by forensic microbiologists from USAMRIID and Lawrence Livermore National Laboratory, and epidemiologists from the CDC.³²⁰

While both types of detectives use similar methods of investigation, the use of their findings is far different. Law enforcement officials protect their information in order to build a case for conviction under the rules of evidence in a court of law. Epidemiologists use different methods and have different goals. They try to figure out what went wrong in a social or physical environment by identifying factors that permit disease to spread. Their goal is to identify and then educate medical and healthcare professionals “so as to increase understanding of the human situation.”³²¹ Education efforts involve the general public, and require the use of media outlets to transmit the message. Police detectives want to review medical records and interview patients, while physicians and medical systems want to protect patient records and their rights to privacy. Police detectives want to guard information and evidence, while epidemiologists want to broadcast and publish information. “When faced with a bioterrorist, however, police detectives and disease detectives share a goal, namely to find and stop the responsible terrorist or group of terrorists.”³²²

3. Forensic Epidemiology and Existing Barriers to Coordination

Public health and law enforcement officials have conducted parallel investigations since the 1970s.³²³ However, the anthrax attacks of 2001 and thousands of associated

³¹⁹ UCLA Department of Epidemiology, *American Anthrax Outbreak*.

³²⁰ Ibid.

³²¹ Fraser, *Epidemiology as a Liberal Art*, 310.

³²² Ibid.

³²³ Richard A. Goodman et al., “Forensic Epidemiology: Law at the Intersection of Public Health and Criminal Investigations,” *Journal of Law, Medicine and Ethics* 31, no. 4 (2003): 684.

hoaxes have required these agencies to work together in unprecedented ways.³²⁴ Suspicions that the West Nile Virus in the United States could have been a deliberate act presented additional challenges for public health and criminal investigators.³²⁵ “The concurrent responses to such threats affirmed the many similarities in the goals and investigative methods used by both law enforcement and public health officials but also highlighted salient differences in the different disciplines’ approaches.”³²⁶ Consequently, a new field emerged called microbial forensics or forensic epidemiology. Forensic epidemiology is “the use of epidemiologic and other public health methods in conjunction with or as an adjunct to an ongoing criminal investigation.”³²⁷ The American Academy of Microbiology says “the emerging discipline...combines principles of public health epidemiology and law enforcement to identify patterns in a disease outbreak, determine the pathogen involved, control its spread and trace the microorganism to its source—the perpetrator(s).”³²⁸

In 2002, the CDC’s Public Health Law Program developed a module for the joint training of public health and law enforcement officials. The goal was and is to “foster improved understanding of the investigative goals and methods specific to each discipline and to strengthen interdisciplinary collaborative effectiveness in response to future attacks.”³²⁹ The joint training module is a self-contained instructional package that can be used in any jurisdiction throughout the United States.³³⁰ The CDC’s *Course Manager’s Guide* and the FBI’s *Criminal and Epidemiological Investigation Handbook*

³²⁴ Centers for Disease Control and Prevention, *Course Managers Guide, Forensic Epidemiology: Joint Training for Law Enforcement and Public Health Officials on Investigative Responses to Bioterrorism* (Washington, D.C.: Department of Health and Human Services, 2004), 1.

³²⁵ The term “forensic epidemiology” was limited to epidemiologists serving as expert trial witnesses prior to 1999. However, in October of that year, former Soviet bioweapon director Dr. Kenneth Alibek first used the term to describe a necessary future investigative capability. His comments were during congressional testimony about the West Nile Virus and whether it could have been deliberate. Goodman et al., *Forensic Epidemiology*, 684.

³²⁶ Centers for Disease Control and Prevention, “Forensic Epidemiology—Program Details,” <http://www2.cdc.gov/phlp/ForensicEpi/Background.asp> (accessed November 16, 2006).

³²⁷ Goodman et al., *Forensic Epidemiology*, 685.

³²⁸ Quoted in Goodman et al., *Forensic Epidemiology*, 685.

³²⁹ Centers for Disease Control and Prevention, *Forensic Epidemiology*.

³³⁰ The course module was piloted at three sites before final revision and national release in spring 2003. These locations were Jacksonville, Florida (December 3-4, 2002), Baltimore, Maryland (December 17-18, 2002), and Los Angeles, California (January 15-16, 2003). Ibid.

are the two primary deliverables that have resulted from collaborative efforts thus far.³³¹ This forensic epidemiology course is currently in a national dissemination mode. As of September 2004 it had been taught in 165 training sessions in 42 states and territories.³³² While the growth of this new field and associated training programs are a step towards increasing attribution of biological attacks, problems of interagency coordination remain.

Barriers to coordination have been identified for both public health and law enforcement agencies. During joint workshops, participants noted two barriers for the sharing of patient information.³³³ First is the public health community's concern that it will be held liable for the release of patient information without consent. Second is the apprehension of sharing sensitive patient information with law enforcement based on issues of ethics and trust. Patients sometimes provide very personal information to healthcare professionals expecting that it will be safeguarded in confidence. Public health officials worry that by sharing such information with law enforcement, regardless of the situation, it will jeopardize their future ability to perform duties as patients begin to withhold information for fear it will be released. It would damage the "doctor-patient" privilege of privacy and violate their professional code of ethics.³³⁴

Two barriers were also noted for the law enforcement community. First, they are reluctant to share information with public health officials because it could "jeopardize the safety of confidential informants or the security of classified sources."³³⁵ Public health officials understand this dilemma, but nonetheless desire "alerts" when a heightened awareness is warranted. Such alerts would permit public health officials "to be on the lookout for unusual or unexplained illnesses, and to monitor what may otherwise initially be overlooked as a signal that there has been a biological release."³³⁶ The second concern of law enforcement officials is that suspects may avoid capture as a result of

³³¹ See <http://www2.cdc.gov/phlp/ForensicEpi/docs/CourseMgrGuide.pdf> for the CDC's *Course Manager's Guide*, and http://www.ecbc.army.mil/downloads/mirp/ECBC_ceih.pdf for the FBI's *Criminal and Epidemiological Investigation Handbook*.

³³² Centers for Disease Control and Prevention, *Forensic Epidemiology*.

³³³ Federal Bureau of Investigation, *Criminal and Epidemiological Investigation Handbook* (Washington, D.C.: Department of Justice, 2003), 3.

³³⁴ *Ibid.*, 5.

³³⁵ *Ibid.*, 6.

³³⁶ *Ibid.*

sharing investigative information. Inadvertent leaks back to the suspect are more likely the more people that have access to investigative data. Unintended tip-offs could give suspects enough time to either destroy evidence or avoid detection altogether.

Finally, experts and experience from bioterrorism training exercises reveals other barriers to coordination.³³⁷ Cindy Lambdin from U.C. Berkeley's School of Public Health, Center for Infectious Disease Preparedness, has observed the same repeated mistakes in her more than 20 years of public health service and as an emergency response exercise planner. When asked what the biggest barrier to coordination is between public health and law enforcement officials, she responded, "They don't speak the same language. They lack a common vocabulary."³³⁸ The word "surveillance" was used as an example. To public health officials, surveillance (of infectious disease) means something quite different than it does to law enforcement officials (in the course of a criminal investigation).

The research literature does not address organizational cultural and its obstruction to the sharing of information between public health and law enforcement agencies. Experts like Mrs. Lambdin suggest that public health's reluctance to notify law enforcement about the potential use of biological agents represents a cultural problem within the community.³³⁹ Public health officials are unwilling to contact law enforcement agencies without positive test results. What is more, often they will wait for not one, but two conclusive tests before initiating any coordination. Unfortunately, biology and nature can not be hastened. Depending on the pathogen, it can literally take weeks to culture some tests to determine the presence of certain agents. Waiting for test results exacerbates the time problem from detection to response shown previously in Figure 8, page 75. Experts believe that for the public health community, the fear of making a false-positive regarding bioterrorism outweighs the fear of making a either late call, or no call at all.

³³⁷ Author interview with Cindy Lambdin at California's annual *Golden Guardian* disaster response exercise, November 15, 2006.

³³⁸ Ibid.

³³⁹ Ibid.

Up to this point, key terms have been defined and findings from the case studies have been synthesized. A notional model of biodefense was introduced based on the primacy of surveillance facilitating detection, and cooperation facilitating attribution. A call for the re-balancing of national biodefense priorities was supported by revealing public health limitations and existing barriers to interagency coordination. This study now concludes by suggesting a future framework of bioterrorism, by considering what previous generations of experts proposed as solutions to the same problem, and by providing specific recommendations to strengthen U.S. biodefense strategy.

V. CONCLUSION

We need to strengthen things. We need to strengthen our public health system, our education, we need to strengthen our laboratory systems. ...We have gaps. We can, indeed, make our response stronger, and it's imperative that we do so.³⁴⁰

Detection and attribution of biological events are dependent variables in a notional model of biodefense. Surveillance facilitates detection, while interagency cooperation facilitates attribution. Research of the U.S. public health system found its organizational structure, laboratory capacity, and National Detection System to be the top three limitations that hinder effective surveillance. The relationship between public health and law enforcement was found to be most vital for achieving attribution. Study of these two communities found that the subtle yet existing differences in the way they manage nature of attack, and the distinct roles they play in the surveillance and epidemiological processes, serve to encumber cooperation and thus attribution.

This chapter concludes first by considering the future bioterrorism threat environment. While circuitously related to BW detection and attribution, the case studies and thesis research support these findings as being imperative for biodefense preparedness and overall national security. Next, the chapter takes a historical look at how previous generations of public health and bioterrorism experts addressed the same problems of today. Finally, these themes are combined with thesis findings to provide policy recommendations for improving detection and attribution capabilities, and therefore strengthen preparedness and U.S. biodefense strategy.

A. THE FUTURE FRAMEWORK OF BIOTERRORISM

Thesis research has revealed that the future bioterrorism threat is different than what most literature on the subject portrays. Therefore, the new challenges facing U.S. biodefense and its implications for national preparedness are now considered. Traditional views of infectious disease and national security have focused on military forces and their ability to survive BW attacks and sustain combat operations. However, a paradigm shift

³⁴⁰ HHS Secretary Tommy Thompson before the Senate Subcommittee on Labor, Health, and Human Services during the U.S. anthrax attacks October 3, 2001. National Defense University, *Anthrax in America*, 20.

has occurred and the emerging link between infectious disease and U.S. national security is now recognized.³⁴¹ Evolving security concepts today acknowledge the potential impacts of disease on general population mortality, economic loss, and social and government disruption.³⁴² These are key drivers for the orientation of U.S. biodefense strategy. Similarly, the research for this thesis has uncovered new challenges facing U.S. biodefense with direct implications for preparedness and national security.

1. Terrorists Are Managing Capabilities³⁴³

The Rajneesh and anthrax cases demonstrate that terrorists are dealing with the requirements of biological weapons in one of two ways. They are either slowly climbing the capabilities curve themselves, or are settling for a substitute capability by attempting to acquire the necessary technology, professional skill, and sensitive materials from others. Whether state or non-state actor, successful programs require four distinct capabilities. These are the means to acquire, to produce, to weaponize (if necessary), and to effectively deliver a biological weapon. History shows that organizations make their agent selection—even sometimes reconsider their operational objectives—based solely on their capabilities in these four areas. History also shows that some terrorists, cults, and apocalyptic groups remain determined to use biological weapons to achieve their strategic objectives. Lastly, recent developments in the ongoing U.S. anthrax investigation show that some may have achieved capabilities that before were considered unattainable.³⁴⁴

Even so, the highly technical skills required for milling and aerosolizing biological materials while at the same time maintaining a virulent strain can be circumvented. Acquisition of the right material, such as a contagious and highly transmittable pathogen with no known cure, completely bypasses the weaponization and

³⁴¹ Cecchine and Moore, *Infectious Disease and National Security*, 15.

³⁴² *Ibid.*, 16-18.

³⁴³ Also see Christopher M. Thompson, “The Bioterrorism Threat by Non-State Actors: Hype or Horror?” (Masters thesis, Naval Postgraduate School, December 2006).

³⁴⁴ Scientific tests at several laboratories counter the widely held belief that the attacks involved a government scientist or person with access to a U.S. biodefense lab. The anthrax powder contained no additives or special process to make it more deadly. “Whoever made the powder produced a deadly project of exceptional purity and quality—up to a trillion spores per gram—but used none of the tricks known to military bioweapons scientists to increase the lethality of the product.” Lengel and Warrick, *FBI Is Casting A Wider Net in Anthrax Attacks*.

delivery problem and can place groups squarely in the mass destruction zone. Therefore, access to advanced biological weapons, certain types of genetically altered DNA, or lethal contagious pathogens present serious nonproliferation concerns. Armed with a transmissible weapon, the human, livestock, or plant host becomes the vector. The technical challenges that constrained Aum Shinrikyo, the Rajneeshees and others are quickly solved. More likely than not, the limited amount of advanced material combined with strict security protocols will force terrorists towards less lethal and destructive agents, driving them down the BW threat curve. While containing attackers in this operating space is a success on the one hand, it poses new challenges for biodefense preparedness on the other. The result is a requirement for quicker detection of inconspicuous disease outbreaks.

2. Mass Effects vs. Mass Destruction

The term “WMD” is grossly overused, is short-sighted and sometimes misapplied, and on the whole represents an old way of thinking.³⁴⁵ The future framework of terrorism demands considering and preparing for the full spectrum of possible devastating effects. Persistent materials like radioisotopes or anthrax spores can deny the use of territory and compel governments into costly cleanup. The isotopes need not be from highly enriched fissile materials, and the spores need not be from a virulent strain. The American public would demand and politicians would be responsible for rendering affected areas safe. Fallout from a dirty bomb or a cloud of anthrax would leave portions of metropolitan cities uninhabitable. The direct costs of decontamination—street by street, and building by building—would be astronomical. The cascading and indirect economic effects from lost productivity, failed businesses, and unrealized future earnings would be additionally enormous. The psychological trauma and degradation of public confidence in the government to protect citizens would be immeasurable. Finally, any resulting amendments or additions to national law, reorganization or creation of governmental agencies, or necessary changes in private or public security practices would also represent further intangible costs. It is not enough to say that such doomsday scenarios are just speculation and have not yet happened. The 1984 Rajneeshee, the 1995 Aum Shinrikyo, and the 2001 anthrax attacks all were only conjecture before becoming

³⁴⁵ Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz, *Planning the Unthinkable: How New Powers Will use Nuclear, Biological, and Chemical Weapons* (Ithaca, NY: Cornell University Press, 2000), 239.

reality. Interestingly the Rajneesh, and in all probability the U.S. anthrax case, convincingly show that attack objectives were not mass destruction or mass casualties.

Another area of concern is the potential cascading effects of bioterrorism that can cripple critical infrastructure. This is important because agriculture offers another avenue for infectious disease to enter human populations via livestock and plant hosts or sources. Avian H5N1 influenza through poultry and the recent *E. Coli* spinach outbreak through U.S. produce are examples.

Accordingly, champions of critical infrastructure protection warn of bioterrorism as a tool to wage sustained economic warfare. U.S. agriculture statistics, the potential impacts on citizens and the national economy, and existing vulnerabilities all combine to present an alarming picture.³⁴⁶ The August 2006 Congressional Research Service report *Agroterrorism: Threats and Preparedness* concludes that agroterrorism is a subset of bioterrorism, defined as the intentional introduction of animal or plant disease to generate fear, cause economic loss, and/or undermine social stability.³⁴⁷ “The goal of agroterrorism is not to kill cows or plants. These are the means to the end of causing economic damage, social unrest, and loss of confidence in government”³⁴⁸ The same logic applies to the public health sector. Its ability to absorb an attack was challenged at both state and local levels by the simple Rajneeshee salad bar contaminations. Had the agent used been lethal, or worse yet a contagious virus, the national public health sector could have been severely crippled. The health sector is vast and diverse, “consisting of state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles.”³⁴⁹ The ability of this system as a whole and our first responders to survive a

³⁴⁶ U.S. agriculture accounts for one-sixth of national Gross Domestic Product which equates to over \$1 trillion a year. As a sector, it is the nation’s largest employer with one in eight working directly in food production. Exports total \$50 billion a year—the largest positive contribution to U.S. trade balance. U.S. farming is the most efficient in the world, enabling Americans to spend less than 11 percent of disposable income on food compared to the global average of 20 to 30 percent. Parker, *Agricultural Bioterrorism*, x.

³⁴⁷ Jim Monke, *Agroterrorism: Threats and Preparedness* (Washington, D.C.: Congressional Research Service, Library of Congress, August 25, 2006), ii, <http://www.nationalaglawcenter.org/assets/crs/RL32521.pdf#search=%22Agroterrorism%3A%20Threats%20and%20Preparedness%202006%22> (accessed October 5, 2006).

³⁴⁸ Ibid.

³⁴⁹ The White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 41.

BW attack, provide continuity of operations, and rebound to acceptable and sustainable levels is paramount. If future attacks aim to disrupt rather than destruct—to slowly erode U.S. economies and social stability—then preparedness entails more sensitive disease detection and attribution abilities.

3. The Limits of Attribution for Dissuasion and Deterrence

Attribution plays a crucial role in the future of dissuading and deterring WMD terrorism, but it is not the mainstay of biodefense preparedness. The September, 2006 *National Strategy for Combating Terrorism* catalogues a six-point plan for denying WMD “to rogue states and terrorist allies who seek to use them.”³⁵⁰ A vital element for deterrence is being able to define the nature and source of a terrorist-employed WMD device.

Should a WMD terrorist attack occur, the rapid identification of the source and perpetrator of an attack will enable our response efforts and may be critical in disrupting follow-on attacks. We will develop the capability to assign responsibility for the intended or actual use of WMD via accurate attribution – the rapid fusion of technical forensic data with intelligence and law enforcement information.³⁵¹

The words “attribute,” “attribution,” or the concept linking intelligence and law enforcement to identify attackers appears nowhere in the previous strategy document published February, 2003. The concept of advertising an attribution capability in order to bolster dissuasion and deterrence of WMD terrorism is a necessary step forward. However, attribution has limits. It will not dissuade the determined terrorist, nor deter the procedurally rational actor whose objectives may in fact be to create chaos or hasten the end of time—groups whose only constituency is God himself, or whose organizational survival is of no real concern. Unfortunately, this lot makes up 75 percent of the non-state actors who have actually used chemical or biological weapons in more

³⁵⁰ The White House, *National Strategy for Combating Terrorism* (Washington, DC: The White House, September 2006), 13-15, <http://www.whitehouse.gov/nsc/nsct/2006/> (accessed November 26, 2006).

³⁵¹ *Ibid.*, 14-15.

than 244 attacks in 26 countries since World War I.³⁵² Furthermore, attribution may not deter terrorists whose objectives are to provoke a retaliatory response and create regional instability.

This thesis defines attribution as a two-level process. The first tier is differentiating between a natural disease outbreak and a malicious attack. Outbreaks must first be detected and characterized as terrorism. While this seems obvious in theory, history and the case studies show it to be more difficult in practice. The second tier is actually tracing back to the perpetrator—the so called ‘return address’ capability. In sum, the Rajneeshee case never got past the first stage to even attempt the second, and underscores the need for effective communication and coordination between intelligence, public health, and law enforcement officials. The first level of attribution relies more heavily on organizational theory than science, is well within our national capabilities, and represents the first line of defense and focus of this thesis.

B. THE 1950s REVISITED

The Epidemic Intelligence Service (EIS) was established in 1951 among heightened fears of biological weapons use against the United States.³⁵³ Following the start of the Korean War, EIS was formed “as an early warning system against biological warfare and man-made epidemics.”³⁵⁴ It was originally composed of doctors, researchers, and scientists who served in 2-year assignments, and today has expanded to also include a surveillance and response unit for epidemics and chronic disease. What is remarkable regarding U.S. vulnerability and preparedness for biological attacks is that the problems in the late 1940s and early 1950s that spawned EIS are much the same today following the 2001 anthrax attacks.

³⁵² Jonathan B. Tucker, “Introduction,” in *Toxic Terror: Assessing Terrorist use of Chemical and Biological Weapons*, ed. Jonathan B. Tucker (Cambridge, MA: MIT Press, 2000), 1.

³⁵³ U.S. and British independent strategic estimates in 1946 were that in future wars, biological weapons were as likely to be used as atomic bombs. These countries assumed the Soviet Union had reached the same conclusion. In May 1947, the testimony of General Ishii Shiro and nineteen other biological warfare specialists confirmed the existence of a Japanese BW program and the atrocities of Detachment 731. A biological arms race resulted that left the United States troubled by its vulnerability and lack of preparedness for biological attacks. Robert Harris and Jeremy Paxman, *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare* (New York, NY: Random House, 2002), 152-6.

³⁵⁴ Centers for Disease Control and Prevention, *Epidemic Intelligence Service*.

In October 1951, before the American Public Health Association, Colonel William L. Wilson of the Federal Civil Defense Administration said, “Biological warfare or ‘BW’ is not new! Biological warfare defense is not a new subject either. This type of warfare, so widely popularized today as a new subject, is one which we propose to clarify from the civil defense viewpoint.”³⁵⁵ Champions of contemporary biodefense find themselves opening with this same argument some 55 years later. Yet what is most telling is the approach and mindset our predecessors took to addressing the problem. Two themes emerged in the 1950s. First was the need for policymakers to take the situation seriously and recognize the BW threat from a civil defense perspective. Second was that all the necessary tools and resources already existed to manage the problem. The following is a series of statements made in 1951, and later published in 1952 that summarize these points.

Once identified, reporting of the agent and the marshalling of defenses against it should be much more rapid than in days gone by, and in our modern civilization the defense measures certainly could be more effective from the earliest attacks, *provided we undertook our problems energetically, prepared for them intelligently, and deployed the means of defense promptly.*

Biological warfare defense is energetic public health practice. ...Surely all of us now realize that *if we really desire to do so*, we can achieve epidemiological investigations which will protect our populations and we can report them promptly and effectively. ...we must agree that we have come a long way toward the goal of means for overcoming any biological agent directed against us, *if we will but prepare intelligently and effectively* for that.

The interrelationships and mutual supports between federal and state and other governmental and professional agencies and groups should be clearly recognized. While *civil defense must coordinate* and assure all of the defense measures required to be used against biological warfare, *the various essential services are available.*

You have heard also of the United States Department of Agriculture’s Animal and Plant Disease Control agencies, and of the Department of Interior’s Fish and Wildlife Service. *We realize and appreciate the*

³⁵⁵ William L. Wilson, “Biological Warfare Defense. 1. Introductory Remarks,” *American Journal of Public Health* 42, no. 3 (March 1952): 233.

*necessity for us to use most intelligently the vast and marvelous resources we have in our country today. ...On the other hand, a very great deal depends upon individuals, each doing his part.*³⁵⁶

The concluding remarks in Judith Miller, Stephen Engelberg, and William Broad's 2001 book titled *Germs: Biological Weapons and America's Secret War* also bear repeating:

A half century ago, a group of eminent citizens warned James Forrestal, the first Secretary of Defense, that the United States was defenseless against germ attacks. But its recommendations for better intelligence, more research, drug stockpiles, and medical surveillance systems were largely ignored. Over the next five decades, a series of American presidents confronted the problem, considering various remedies, and shuffled the issue in the "too hard" box. Such denial is understandable. Biodefense has no natural political constituency in Washington. The military-industrial complex that supports weapons systems has little interest in vaccines and public health.

"Plans should be prepared for the establishment of adequate laboratories and vaccine production facilities and stockpiles of essential basic medical supplies in the event the danger from enemy attack appears immanent," Forrestal's committee concluded in 1949. "Prompt action should be taken to establish a civil defense program."

Those words could have been written yesterday. The question is whether the United States will be able to wait another fifty years to act on them. If we as a nation believe that the germ threat is a hoax, we are spending too much money on it. But if the danger is real, as we conclude it is, then the investment is much too haphazard and diffuse. We remain woefully unprepared for a calamity that would be unlike any this country has ever experienced.³⁵⁷

The father of EIS, Dr. Alexander D. Langmuir, also concluded in 1952 that "sound organization can do much to abort the attack or mitigate its serious consequences. ...The defensive organization is already in existence (in our health departments) and needs only modification to meet unnatural outbreaks or disease."³⁵⁸ Langmuir spoke of the need to increase the number of trained epidemiologists, to have an alert and effective

³⁵⁶ Italics added for emphasis. Ibid., 233-4.

³⁵⁷ Miller, Engelberg and Broad, *Germs*, 320.

³⁵⁸ Alexander D. Langmuir and Justin M. Andrews, "Biological Warfare Defense. 2. The Epidemic Intelligence Service of the Communicable Disease Center," *American Journal of Public Health* 42, no. 3 (March 1952): 235.

laboratory system, to have physicians and first responders trained in identifying the signs of bioterrorism, to have “a sound intelligence system based on prompt morbidity reporting,” and to have effective relationships between public health and law enforcement to characterize and attribute BW attacks.³⁵⁹ Such are also the findings of this thesis more than a half-century later.

Building scientific laboratories for defensive biological research like the National Biodefense Analysis and Countermeasures Center, and creating an atmosphere of opacity versus transparency by classifying the work in the name of national security, while at the same time rejecting Biological and Toxin Weapons Convention (BWC) protocols in the name of freedom and economic prosperity make for a dismal and counterproductive biodefense strategy.³⁶⁰ Regarding the BWC, “The United States undermines the treaty it helped create and its own moral authority when it cloaks the most significant aspects of its defensive work in secrecy. ...A balance can be struck between the need to protect legitimate research and the imperative of investigating cheaters.”³⁶¹

As in the 1950s, the time has come once again to place increased emphasis on the ominous threat of bioterrorism. Yet it must be done smartly to be effective and increase national preparedness. While the defense establishment has a role to play, the majority of vulnerabilities and drivers for national security concern do not lie there. U.S. biodefense strategy is more a civil defense concern as the future framework threatens general populations, global economies, and social stability and continuity of government. Determining the threat level and placing relative dangers in perspective is important.³⁶² However, if policymakers do this, and then collectively decide we must “do something,” then we must take measures that truly enhance security.

³⁵⁹ Langmuir and Andrews, *Biological Warfare Defense*, 235-7.

³⁶⁰ For issues relating to the United State and its reluctance to accept BWC inspection protocols see Barletta et al., *Keeping Track of Anthrax*, Barletta, *Assessing Risks and Crafting Responses*, 71-2, and Harris and Paxman, *A Higher Form of Killing*, 252. For concerns about the NBACC and research transparency see Shea, *The National Biodefense Analysis and Countermeasures Center*, CRS-1, and Joby Warrick, “Tight lid kept on new U.S. bioterror facility,” *The Seattle Times*, August 1, 2006, http://seattletimes.nwsources.com/html/nationworld/2003166525_bioterror01.html (accessed November 26, 2006).

³⁶¹ Miller, Engelberg and Broad, *Germes*, 317-9.

³⁶² Parachini, *Anthrax Attacks*, 10.

The biodefense arguments half a century ago still hold today. Sometimes the best solutions are also the simplest and least costly—to improve organizational efficiency, communication, and coordination. To build trusted networks and place value on the power of professional and personal relationships. To enhance training and exercise programs for existing personnel, and to fix and better use current resources, rather than build new ones and create more bureaucracy at a higher price. To improve BW detection through better surveillance, and to improve attribution through better interagency coordination. We must learn the right lessons from history and bioterrorism case studies to properly allocate valuable resources and truly improve national preparedness. Otherwise, the United States could find itself 55 years from now revisiting the lessons of today.

C. RECOMMENDATIONS

1. Improve Detection Through Better Surveillance

Detecting bioterrorism requires vigilant and effective surveillance. Better surveillance requires more uniformity across state systems, an increase in the public health workforce and laboratory capacity, mandatory versus voluntary disease reporting, and stronger oversight mechanisms to ensure improvement and compliance in all of these areas.³⁶³ More systems like the National Biosurveillance Integration System (NBIS)—which use active surveillance at lower operational costs by leveraging data already collected for other means—should be developed and fielded. Finally, consideration should be given to the sharing of any testing technologies between the defense establishment and state and local laboratories.

Some states have enhanced their surveillance systems, but improvements have not been uniform across the country.³⁶⁴ In 2004, only half of states reported that their health departments could *continuously* receive and evaluate reports, and few reported the ability to rapidly detect an outbreak of an influenza-like illness. In addition, few have links between public health, livestock, and veterinary surveillance communities to monitor

³⁶³ For a complete tutorial on the U.S. “biodefense workforce crisis,” see Partnership for Public Service, “Homeland Insecurity: Building the Expertise to Defend America from Bioterrorism,” http://www.ourpublicservice.org/research/research_show.htm?doc_id=181630 (accessed November 26, 2006).

³⁶⁴ General Accounting Office, *Public Health Preparedness: Response Capacity Improving, but Much Remains to be Accomplished* (Washington, D.C.: General Accounting Office, February 12, 2004), 5.

diseases in animals that may be spread to humans (zoonosis), such as the West Nile virus.³⁶⁵ While the principle of federalism and differences in state constitutions and laws are understandable, it also stands to reason that a deadly outbreak in any state could have devastating national effects. If one truly believes the common adage “disease knows no borders,” then the federal government should ensure capacity and uniformity across state surveillance systems.

Both the Rajneesh and anthrax cases show that during bioterror events, surges from hoaxes, normal testing, and “the worried well” immediately combine to overwhelm laboratories. As of February 2004, some states have increased their capacity to perform tests, but this has not been consistent across the nation.³⁶⁶ All states participate in the CDC Laboratory Response Network, but only half have at least one public health laboratory with the appropriate equipment and trained staff to test and identifying biological agents. Additionally, only half have a facility with the biosafety level required to handle agents such as anthrax. Uniform efforts should be made to increase each state’s trained workforce and laboratory surge capacity, and to provide a BSL-3 facility in every state.³⁶⁷

The list of nationally notifiable diseases is updated annually. The CDC has also recommended detailed reporting standards via the “8-City Enhanced Terrorism Surveillance Project.”³⁶⁸ Yet much of disease surveillance reporting remains

³⁶⁵ General Accounting Office, *Public Health Preparedness*, 5.

³⁶⁶ Ibid.

³⁶⁷ Since the anthrax attacks federal money through CDC grants has permitted states to appoint an Executive Director of Bioterrorism Preparedness and response, to designate a response coordinator, and to hire at least one epidemiologist for each metropolitan area with a population greater than 500,000. However, most still report staffing concerns and find it difficult to hire epidemiologists and laboratory technicians. Workforce shortages in these areas are described by many states to be a long-term challenge for preparedness. Ibid., 6-7.

³⁶⁸ CDC guidance is called *Performance Criteria for Public Health Disease Reporting Systems Operating Twenty-four Hours per Day, Seven Days per Week (24/7)*, and can be viewed at http://www.cdc.gov/epo/dphsi/files/Performance_Criteria_Public_Health_Disease_Reporting_Systems.doc (accessed November 22, 2006).

voluntary.³⁶⁹ Sensitivity levels should be lowered, and more reporting requirements be made mandatory, in order to improve national preparedness for outbreaks of naturally occurring infectious disease or biological attacks.

State legislatures must assume stronger oversight of regional and local health departments, while Congress should assume stronger oversight of state surveillance systems without politicizing their agencies. This should come by way of both scheduled and random site visits and exercises. CDC and the Health Resources and Services Administration (HRSA) do visit state and local health departments to ensure grant monies are spent properly.³⁷⁰ However, these inspections are for very limited and focused concerns, sometimes unrelated to disease surveillance and detection. The federal government should hold states, and states should hold local public health departments, accountable for surveillance and detection performance. Oversight mechanisms should focus on standardization and conformity to state and national procedures, the adequacy of workforce and laboratory capacity, and compliance with mandatory reporting requirements within specified timelines.

More systems like NBIS should be developed and fielded. These reduce the costs of active surveillance by using existing data that is already routinely collected for other purposes. This eliminates the need to develop and maintain more special purpose data collection systems. Value-of-information considerations can also be used to reduce costs even further. This decision theory principle determines the utility of whether to collect

³⁶⁹ “In 1878, Congress authorized the U.S. Marine Hospital Service...to collect morbidity reports regarding cholera, smallpox, plague, and yellow fever from U.S. consuls overseas...The authority for weekly reporting and publication of these reports was expanded by Congress in 1893 to include data from states and municipal authorities. To increase the uniformity of the data, Congress enacted a law in 1902 directing the Surgeon General to provide forms for the collection and compilation of data and for the publication of reports at the national level. In 1912, state and territorial health authorities...recommended immediate telegraphic reporting of five infectious diseases and the monthly reporting, by letter, of 10 additional diseases...By 1928, all states, the District of Columbia, Hawaii, and Puerto Rico were participating in national reporting of 29 specified diseases. At their annual meeting in 1950, the State and Territorial Health Officers authorized a conference of state and territorial epidemiologists whose purpose was to determine which diseases should be reported...In 1961, CDC assumed responsibility for the collection and publication of data concerning nationally notifiable diseases.” Centers for Disease Control and Prevention, “National Notifiable Diseases Surveillance System,” <http://www.cdc.gov/epo/dphsi/nndsshis.htm> (accessed November 22, 2006).

³⁷⁰ Author interview with Cindy Lambdin at California’s annual *Golden Guardian* disaster response exercise, November 15, 2006. HRSA is an agency of the U.S. Department of Health and Human Services with the mission to provide “national leadership, program resources and services needed to improve access to culturally competent, quality health care.” See <http://www.hrsa.gov/about/default.htm> (accessed November 22, 2006).

certain kinds of information.³⁷¹ Data mining principles can and should be used to probe web-based sources in both the secure and non-secure realms to enhance overall disease surveillance.

Finally, consideration should be given to the sharing of any testing technologies from USAMRIID and the newly established NBACC with state and local laboratories.³⁷² If classified technologies or advanced scientific testing procedures do exist within DoD, these should be scrutinized and their classification reconsidered. Thought should be given to sharing such capabilities (if they exist) with state laboratories to accelerate traditional growth culture testing. This would speed up the detection timeline at state and local levels—the first line of defense where more than 66 percent of cases are detected and reported.³⁷³

2. Improve Attribution through Better Coordination and Information Sharing³⁷⁴

More bureaucracy is not the answer to improve interagency coordination. New agencies, departments, and duty titles will not further BW attribution. This was well understood in the 1950s when leading experts insisted that most of the tools and services needed were already in place.³⁷⁵ It is still true today when authorities maintain that “extraordinary measures are not necessary” to address this problem.³⁷⁶ Rather than more layers of bureaucracy, trusted networks should be developed from existing organizational structures by using “the strength of weak ties.”³⁷⁷

The strength of weak ties is an organizational theory principle that says personal relationships or loose connections between organizations create more and shorter paths of

³⁷¹ Wagner et al., *The Nation's Current Capacity*, 50.

³⁷² Author interview with Cindy Lambdin at California's annual *Golden Guardian* disaster response exercise, November 15, 2006.

³⁷³ Ashford et al., *Planning against Biological Terrorism*, 515.

³⁷⁴ See Clunan, *Building Trusted Networks for Attributing Use of Biological Agents*.

³⁷⁵ Wilson, *Biological Warfare Defense*, 233 and Langmuir and Andrews, *Biological Warfare Defense*, 235.

³⁷⁶ Department of Health and Human Services, *The Public Health Response*, 15.

³⁷⁷ Mark S. Granovetter, “The Strength of Weak Ties,” *American Journal of Psychology* 78, no. 6 (May 1973): 1360.

communication.³⁷⁸ This suggests that where interagency coordination is concerned, “removal of the average weak tie would do more ‘damage’ to transmission probabilities than would that of the average strong one.”³⁷⁹ Information can reach more people and traverse greater social distance when passed through weak ties rather than strong ones. Weak ties also play a role in promoting social cohesion, and this is especially true in professional and technical specialties that are well defined and restricted in size.³⁸⁰ Furthermore, when people transfer from one organization to another, they often maintain working relationship established in the previous network, and bring these with them into the new network.

...mobility [from changing jobs] sets up elaborate structures of bridging weak ties...that constitute operative networks in particular locations. Information and ideas thus flow more easily through the specialty, giving it some ‘sense of community,’ activated at meetings and conventions. Maintenance of weak ties may well be the most important consequence of such meetings.³⁸¹

The ability of weak ties to promote disease surveillance and detection was demonstrated in the successful identification of Severe Acute Respiratory Syndrome (SARS) in 2003. Dr. Stephen O. Cunnion, a retired outbreak specialist from the U.S. Navy, posted an e-mail on the International Society for Infectious Disease *ProMED* web site after hearing of suspicious events from friends in China.³⁸² A copy of his original message follows:

³⁷⁸ Granovetter, *The Strength of Weak Ties*, 1365.

³⁷⁹ Ibid., 1366.

³⁸⁰ Ibid., 1373.

³⁸¹ Ibid.

³⁸² ProMED is “the global electronic reporting system for outbreaks of emerging infectious diseases and toxins, open to all sources. ProMED–mail, the Program for Monitoring Emerging Diseases, is a program of the International Society for Infectious Diseases.” International Society for Infectious Diseases, “ProMED–mail,” <http://www.isid.org/> (accessed November 30, 2006). Also see Donald G. McNeil and Lawrence K. Altman, “As SARS Outbreak Took Shape, Health Agency Took Fast Action,” *The New York Times*, Section 1, Column 1, Foreign Desk, May 4, 2003, <http://query.nytimes.com/gst/fullpage.html?sec=health&res=9A0CE2D7123CF937A35756C0A9659C8B63> (accessed November 30, 2006).

PNEUMONIA - CHINA (GUANGDONG): RFI

A ProMED-mail post

<<http://www.promedmail.org>>

ProMED-mail is a program of the
International Society for Infectious Diseases
<<http://www.isid.org>>

Date: 10 Feb 2003

From: Stephen O. Cunnion, MD, PhD, MPH <cunnion@erols.com>

This morning I received this e-mail and then searched your
archives and found nothing that pertained to it. Does anyone know
anything about this problem?

"Have you heard of an epidemic in Guangzhou? An acquaintance of
mine from a teacher's chat room lives there and reports that the
hospitals there have been closed and people are dying."

Stephen O. Cunnion, MD, PhD, MPH
International Consultants in Health, Inc
Member ASTMandH, ISTM³⁸³

This warning and similar queries started a sequence of events that eventually led to the successful management of the SARS epidemic. Examples such as these show the value and power of personal relationships and weak ties. These should be reinforced to promote collaborative networks and improve BW attribution.

Communication among networks is based on trust.³⁸⁴ When it comes to sharing information between organizations, trust and mutual respect are critical and necessary components. In the GAO report *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, all organizations studied identified trust as "the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships."³⁸⁵ Other factors critical to the successful information sharing were:

³⁸³ International Society for Infectious Diseases, "ProMED—mail,"
http://www.promedmail.org/pls/promed/f?p=2400:1202:3322735090787711471::NO::F2400_P1202_CHECK_DISPLAY,F2400_P1202_PUB_MAIL_ID:X,20658 (accessed November 30, 2006).

³⁸⁴ General Accounting Office, *Information Sharing: Practices that Can Benefit Critical Infrastructure Protection* (Washington, D.C.: General Accounting Office, October 2001), 7.

³⁸⁵ *Ibid.*, 2.

- Creating effective and secure communication mechanisms such as regular meetings and secure web sites,
- Obtaining support of senior managers regarding the sharing of sensitive information and the dedication of resources, and
- Ensuring organizational leadership continuity.³⁸⁶

The CDC and its “PulseNet,” “Epidemic Information Exchange,” and “Data Web” information exchange systems were instrumental to the findings of this study.³⁸⁷

Programs should be developed that promote a culture of collaboration between the public health and law enforcement communities to improve attribution. Worker exchange programs between CDC and FBI, between local public health departments, the coroner, and the sheriff’s department; and opportunities for state and local public health department employees to visit and/or briefly work at CDC are examples. Obviously, long-term worker exchanges (more than just days or a few weeks) would be limited to non-technical specialties, and the administrative details of pay and benefits, security clearances, and lines of authority are beyond the scope of this thesis. Lastly, to be truly effective each community’s organizational culture would have to support these exchange tours as a competitive and career advancing opportunity from the highest levels. Where the CDC and FBI are concerned, the agency’s top employees should compete and be the first selected to promote such programs as career enhancing. Where state and local health departments are concerned, some form of certification should accompany completion of exchange tours, and possibly even eligibility for additional federal funding for departments with graduates of the program.

Finally, meetings such as conferences, seminars, and working groups should be routinely held that assemble public health and law enforcement personnel to exchange ideas on how to improve information sharing, joint investigation, and BW attribution. These meeting should be tailored to executive leadership, as well as management and lower-level workers and they should be multi-jurisdictional as much as possible. The federal government and states should define mandatory minimum participation for their public health and law enforcement employees. Minutes and findings should be recorded

³⁸⁶ General Accounting Office, *Information Sharing*, 2.

³⁸⁷ *Ibid.*, 24-6.

and shared, and funding incentives could be tied to participation. Collectively, worker exchange programs and joint conferences or working groups can form “weak ties” and build trust between organizations that will improve BW attribution through better coordination.

3. Conduct Realistic Training and Large-Scale Exercises

Realistic training teaches the probable yet subtle signatures of biological events to those most likely on the front lines of defense (Figure 7, page 72).

Many terrorism events would not be identified in the high profile, sudden-impact manner that most emergencies are portrayed. Instead, the observant physician, veterinarian, laboratory technician, surveillance data entry clerk, etc., who recognizes an unusual illness or cluster of illnesses or increases in requests for medical services or a specific diagnosis, will most likely be the first to identify the event. For this reason, training of all personnel associated with public health surveillance should be a priority of terrorism response preparedness.³⁸⁸

Some have argued for decades of the need for increased training to improve disease surveillance and detection. In 1952, Alexander D. Langmuir said, “It is obvious that a substantial increase in the number of trained and experienced epidemiologists will be required...”³⁸⁹ That same year John M. Hepler called for the training of sanitation personnel in epidemiological procedures, and to establish close ties with the communicable disease control officer, because “those health workers closest to the population will be the first to hear of any changes occurring in the population or the environment.”³⁹⁰ In October 1999 and before the U.S. anthrax attacks, former Soviet bioweapons engineer Dr. Kenneth Alibek testified before Congress saying:

We must first be able to identify that an attack has occurred. This involves developing equipment...as well as providing training to hospital and health department personnel in recognizing and reporting the signs of a biological attack.³⁹¹

³⁸⁸ Department of Health and Human Services, *The Public Health Response*, 15.

³⁸⁹ At the time, Alexander Langmuir was Officer in Charge of the precursor to the CDC—the Communicable Disease Center of the Public Health Service, Federal Security Agency. Langmuir and Andrews, *Biological Warfare Defense*, 236.

³⁹⁰ John M. Hepler, “Biological Warfare Defense. 3. The State Sanitary Engineer’s Viewpoint,” *American Journal of Public Health* 42, no. 3 (March 1952): 239.

³⁹¹ Federation of American Scientists, “Testimony of Dr. Kenneth Alibek, Chief Scientists at Hardon, Inc.,” http://www.fas.org/irp/congress/1999_hr/99-10-20alibek.htm (accessed November 24, 2006).

After the attacks in December 2001, Alibek reaffirmed his position by saying, “We need to do many things in terms of our preparedness, our possible response, training people...”³⁹² Therefore, to maximize preparedness states should train state and local public health staff in health surveillance, epidemiology, outbreak investigation, and worker biosafety issues. Training must be coordinated with other federal, state, and local health programs “to ensure integration of bioterrorism preparedness and response activities.”³⁹³

Frequent joint (public health and law enforcement) and multi-jurisdictional bioterrorism exercises should be accomplished. The federal government should require states, and states should require their counties and cities, to perform these exercises annually at a minimum. While federal and state-wide emergency response exercises do exist today such as the national Top Officials (TOPOFF) and California’s Golden Guardian exercises, these are broader in objective. Table-top and operational exercises that explicitly test disease surveillance, reporting, detection, and attribution both within and across jurisdictional boundaries should be considered. The federal government and states should publish and make results a matter of public record, and additional funding should be tied to superior performance as an incentive.

Besides the obvious benefits of training and exercises, these programs work to build trust and form lasting relationships of weak ties as described earlier. Joint training such as the forensic epidemiology course provides opportunities for public health and law enforcement to collaborate and become familiar with one another’s strengths and weaknesses. Business cards are exchanged and friendships made during operational and table-top exercises. Joint training programs and exercises, therefore, provide the synergistic effect of building trusted networks while at the same time increasing biodefense preparedness.

³⁹² Alibek, *Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons*, 70.

³⁹³ Department of Health and Human Services, *The Public Health Response*, 12.

In summary, a comprehensive national biodefense strategy should make little distinction between mitigating the spread of naturally occurring infectious disease or malicious terrorist attacks. Whether H5N1 bird flu, salmonella, or weaponized anthrax; successful consequence management of biological incidents requires many of the same policies, programs, infrastructure, organization, and training in order to be effective. If we are to learn the right lessons from history and draw the correct conclusions from previous bioterror events, then genuine preparedness requires looking beyond new research facilities and government pharmaceutical contracts. It requires an honest and introspective look within toward existing agencies and available resources. It calls for seriously reconsidering U.S. policy toward BWC inspection protocols—a move that would be more consistent with nonproliferation and signal U.S. international leadership in step with, rather than counter to, its stated biodefense policies. Finally, and above all, it demands improving biological detection and attribution capabilities through better surveillance and interagency cooperation in order to increase preparedness and close existing gaps in U.S. biodefense strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Anderson, P. "The Rajneeshee Cult." Passagen, <http://hem.passagen.se/jan.olofsson/biowarfare/history/rajneeshee.html> (accessed September 20, 2006).
- Answers.com. "Rajneesh." <http://www.answers.com/topic/rajneesh> (accessed September 20, 2006).
- Ashford, David A., Robyn M. Kaiser, Michael E. Bales, Kathleen Shutt, Amee Patrawalla, Andre McShan, Jordan W. Tappero, Bradley A Perkins, and Andrew L. Dannenberg. "Planning against Biological Terrorism: Lessons from Outbreak Investigations." *Emerging Infectious Disease* 9, no. 5 (May 2003): 515-519.
- Barletta, Michael, Amy Sands, and Jonathan B. Tucker. "Keeping Track of Anthrax: The Case for a Biosecurity Convention." *Bulletin of the Atomic Scientists* 58, no. 3 (May-June 2002): 57-62. http://www.thebulletin.org/article.php?art_ofn=mj02barletta (accessed September 20, 2006).
- Barletta, Michael. "Assessing Risks and Crafting Responses." *Center for Nonproliferation Studies Occasional Papers* 65, no. 8 (May 2002), <http://www.isn.ethz.ch/pubs/ph/details.cfm?v21=73370andid=14675> (accessed October 2, 2006).
- Biotechnology Industry Organization. "House Moves to Shore Up Nation's Biodefenses by Passing BARDA Bill." <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104andSTORY=/www/story/09-28-2006/0004441946andEDATE=> (accessed November 8, 2006).
- Borio, Luciana, Dennis Frank, Venkat Mani, Carlos Chiriboga, Michael Pollanen, Mary Ripple, Syed Ali, Constance DiAngelo, Jacqueline Lee, Jonathan Arden, Jack Titus, David Fowler, Tara O'Toole, Henry Masur, John Bartlett and Thomas Inglesby. "Death Due to Bioterrorism-Related Inhalational Anthrax: Report of Two Patients." *The Journal of the American Medical Association* 286, no. 20 (November 28, 2001), <http://www.ph.ucla.edu/epi/bioter/joc11802.pdf> (accessed March 1, 2006).
- Buehler, James W., Ruth L. Berkelman, David M. Hartley, and Clarence J. Peters. "Syndromic Surveillance and Bioterrorism-Related Epidemics." *Emerging Infectious Diseases* 9, no. 10 (September 23, 2003), <http://www.cdc.gov/ncidod/EID/vol9no10/03-0231.htm> (accessed October 15, 2006).
- Butler, Jay, Mitchell L. Cohen, Cindy R. Friedman, Robert M. Scripp, and Craig G. Watz. "Collaboration between Public Health and Law Enforcement: New Paradigms and Partnerships for Bioterrorism Planning and Response." *Emerging Infectious Diseases* 8, no. 10 (October 2002), <http://www.cdc.gov/ncidod/EID/vol8no10/02-0400.htm> (accessed February 28, 2006).

- Cable News Network. "FDA: E. Coli Linked to Natural Selection Foods." CNN.com. <http://www.cnn.com/2006/HEALTH/09/15/tainted.spinach.ap/index.html> (accessed September 27, 2006).
- Carus, Seth W. *Bioterrorism and Biocrimes: The Illicit use of Biological Agents since 1900*. Washington, D.C.: National Defense University, February 2001. http://www.ndu.edu/centercounter/Full_Doc.pdf (accessed December 7, 2006).
- . "The Rajneeshees (1984)." In *Toxic Terror: Assessing Terrorist use of Chemical and Biological Weapons*, edited by Jonathan B. Tucker, 115-137. Cambridge, MA: MIT Press, 2000.
- Cecchine, Gary and Melinda Moore. *Infectious Disease and National Security*. Santa Monica, CA: RAND National Defense Research Institute, 2006.
- Centers for Disease Control and Prevention. "Avian Influenza: Current Situation." <http://www.cdc.gov/flu/avian/outbreaks/current.htm> (accessed September 27, 2006).
- . *Course Managers Guide, Forensic Epidemiology: Joint Training for Law Enforcement and Public Health Officials on Investigative Responses to Bioterrorism*. Washington, D.C.: Department of Health and Human Services, 2004.
- . "Epidemic Intelligence Service—About EIS." <http://www.cdc.gov/eis/about/about.htm> (accessed November 25, 2006).
- . "Forensic Epidemiology—Program Details." <http://www2.cdc.gov/phlp/ForensicEpi/Background.asp> (accessed November 16, 2006).
- . "Laboratory Network for Biological Terrorism." <http://www.bt.cdc.gov/lrn/biological.asp> (accessed December 19, 2005).
- . "Multiple States Investigating a Large Outbreak of E. Coli O157:H7 Infections." Health Alert Network. <http://www2a.cdc.gov/HAN/ArchiveSys/ViewMsgV.asp?AlertNum=00249> (accessed November 16, 2006).
- . "National Notifiable Diseases Surveillance System." <http://www.cdc.gov/epo/dphsi/nndsshis.htm> (accessed November 22, 2006).
- Chyba, Christopher. "Toward Biological Security." *Foreign Affairs* 81, no. 3 (May–June 2002): 122-136.
- Clunan, Anne L. "Building Trusted Networks for Attributing Use of Biological Agents." Paper presented at the Conference on Identification, Characterization, and Attribution of Biological Weapons Use, Center for Contemporary Conflict, U.S. Naval Postgraduate School and Kings College London, London, U.K., July 12-13, 2006.

- CNW TELBEC. "Achaogen Awarded \$24.7M Biodefense Contract by DTRA." <http://www.cnw.ca/fr/releases/archive/October2006/24/c4159.html> (accessed November 8, 2006).
- Committee on International Relations. *Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons*. Serial No. 107-56. One Hundred Seventh Congress, First Session, December 5, 2001. http://commdocs.house.gov/committees/intlrel/hfa76481.000/hfa76481_0f.htm (accessed October 22, 2006).
- Department of Health and Human Services. "Anthrax: What You Need to Know." Centers for Disease Control and Prevention. <http://www.bt.cdc.gov/agent/anthrax/needtoknow.asp> (accessed February 28, 2006).
- . "HHS Fact Sheet: Project BioShield." <http://www.hhs.gov/news/press/2004pres/20040721b.html> (accessed December 16, 2005).
- . "PHIN: BioSense." Centers for Disease Control and Prevention. <http://www.cdc.gov/phinf/component-initiatives/biosense/> (accessed December 16, 2005).
- . *The Public Health Response to Biological and Chemical Terrorism: Interim Planning Guidance for State Public Health Officials*. Atlanta, GA: Centers for Disease Control and Prevention, July 2001. <http://www.bt.cdc.gov/Documents/Planning/PlanningGuidance.PDF> (accessed March 28, 2006).
- Department of Homeland Security. *BioWatch: Early Detection, Early Response*. Washington, D.C.: Science and Technology Directorate. <http://www.milnet.com/wh/DoHS/BioWatchFactSheetFINAL.pdf> (accessed December 16, 2005).
- . *National Response Plan*. Washington, D.C.: Department of Homeland Security, May 25, 2006. http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml (accessed November 11, 2006).
- Elias, Paul. "BioShield Dispute Underscores Problems with Defense Program." *The Mercury News*. http://www.mercurynews.com/mld/mercurynews/news/breaking_news/15590348.htm (accessed November 8, 2006).
- Falkenrath, Richard A., Robert D. Newman, and Bradley A. Thayer. *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*. Cambridge, MA: BCSIA Studies in International Security, MIT Press, 1998.

- Federal Bureau of Investigation. "Amerithrax: The Search for Anthrax."
<http://www.fbi.gov/anthrax/searchant.htm> (accessed November 27, 2005).
- . *Criminal and Epidemiological Investigation Handbook*. Washington, D.C.: Department of Justice, 2003.
- Federation of American Scientists. "Testimony of Dr. Kenneth Alibek, Chief Scientists at Hardon, Inc." http://www.fas.org/irp/congress/1999_hr/99-10-20alibek.htm (accessed November 24, 2006).
- Fraser, David W. "Epidemiology as a Liberal Art," *The New England Journal of Medicine* 316, no. 6 (February 5, 1987): 309-314.
- Fraser, Susan L. "Enterobacter Infections." EMedicine, August 6, 2006.
<http://www.emedicine.com/MED/topic678.htm> (accessed November 27, 2006).
- General Accounting Office. *Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies*. Washington, D.C.: General Accounting Office, 2003.
<http://www.gao.gov/new.items/d03139.pdf> (accessed November 27, 2005).
- . *Homeland Security: CDC's Oversight of the Select Agent Program*. Washington, D.C.: General Accounting Office, 2002.
<http://www.gao.gov/new.items/d03315r.pdf> (accessed November 27, 2005).
- . *Information Sharing: Practices that Can Benefit Critical Infrastructure Protection*. Washington, D.C.: General Accounting Office, October 2001.
- . *Public Health Preparedness: Response Capacity Improving, but Much Remains to be Accomplished*. Washington, D.C.: General Accounting Office, February 12, 2004.
- Genetic Engineering News. "DOR Biopharma Awarded \$5.3M to Advance Ricin Toxin and Botulinum Toxin Vaccine Programs."
<http://www.genengnews.com/news/bnitem.aspx?name=6256619> (accessed November 8, 2006).
- Global Security Newswire. "Inconclusive Test Results Cited in Delayed Tularemia Notification to Federal, Local Health Agencies."
http://www.nti.org/d_newswire/issues/2005/10/5/35653f39-93ee-416f-9540-a8cc79aaf652.html (accessed December 20, 2005).
- Goodman, Richard A., Judith W. Munson, Kim Dammers, Zita Lazzarini, and John P. Barkley. "Forensic Epidemiology: Law at the Intersection of Public Health and Criminal Investigations." *Journal of Law, Medicine and Ethics* 31, no. 4 (2003): 684-700.

- Granovetter, Mark S. "The Strength of Weak Ties." *American Journal of Psychology* 78, no. 6 (May 1973): 1360-1380.
- Harris, Robert and Jeremy Paxman. *A Higher Form of Killing: The Secret History of Chemical and Biological Warfare*. New York, NY: Random House, 2002.
- Hepler, John M. "Biological Warfare Defense. 3. The State Sanitary Engineer's Viewpoint." *American Journal of Public Health* 42, no. 3 (March 1952): 239-40.
- House Committee on Government. *Terrorism Preparedness*.
<http://www.fbi.gov/congress/congress02/mefford040202.htm> (accessed February 28, 2006).
- International Society for Infectious Diseases. "ProMED—mail." <http://www.isid.org/> (accessed November 30, 2006).
- Internet Movie Database. "Biography for Ken Alibek."
<http://www.imdb.com/name/nm1985907/bio> (accessed October 22, 2006).
- Jenkins, Brian M. "International Terrorism: A New Mode of Conflict." In *International Terrorism and World Security*, edited by David Carlton and Carlo Schaerf. London: Croom Helm, 1975.
- . "Will Terrorists Go Nuclear?" *Orbis* 29, no. 3 (1985): 507-16.
- Jernigan, John A., David S. Stephens, David A. Ashford, Carlos Omenaca, Martin S. Topiel, Mark Galbraith, Michael Tapper, Tamara L. Fisk, Sherif Zaki, Tanja Popovic, Richard F. Meyer, Conrad P. Quinn, Scott A. Harper, Scott K. Fridkin, James J. Sejvar, Colin W. Shepard, Michelle McConnell, Jeannette Guarner, Wun-Ju Shieh, Jean M. Malecki, Julie L. Gerberding, James M. Hughes, and Bradley A. Perkins, "Bioterrorism-related Inhalational Anthrax: The First 10 Cases Reported in the United States," *Journal for Emerging Infectious Diseases* 7, no. 6 (November-December 2001): 933-944. <http://www.cdc.gov/ncidod/EID/vol7no6/pdf/jernigan.pdf> (accessed December 3, 2005).
- Langmuir, Alexander D. and Justin M. Andrews. "Biological Warfare Defense. 2. The Epidemic Intelligence Service of the Communicable Disease Center," *American Journal of Public Health* 42, no. 3 (March 1952): 235-8.
- Lavoy, Peter R., Scott D. Sagan, and James J. Wirtz. *Planning the Unthinkable: How New Powers Will use Nuclear, Biological, and Chemical Weapons*. Ithaca, NY: Cornell University Press, 2000.
- Leitenberg, Milton. *Assessing the Biological Weapons and Bioterrorism Threat*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, December 2005.

- . *Biological Weapons and “Bioterrorism” in the First Years of the 21st Century*. College Park, MD: Center for International and Security Studies, School of Public Affairs, April 2003.
- Lengel, Allan and Joby Warrick. “FBI is Casting a Wider Net in Anthrax Attacks.” Washingtonpost.com. <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/24/AR2006092401014.html> (accessed October 5, 2006).
- Levy, Barry S. and Victor W. Sidel. *Terrorism and Public Health: A Balanced Approach to Strengthening Systems and Protecting People*. New York: Oxford University Press, 2003.
- Lister, Sarah A. *An Overview of the U.S. Public Health System in the Context of Emergency Preparedness*. Washington, D.C.: Congressional Research Service, March 17, 2005.
- Loonsk, John W. “BioSense—A National Initiative for Early Detection and Quantification of Public Health Emergencies.” *Morbidity and Mortality Weekly Report* 53, Supplement (September 24, 2004): 53-55, <http://www.cdc.gov/MMWR/preview/mmwrhtml/su5301a13.htm> (accessed December 16, 2005).
- Manning, Stephen. “Hospital Sued by Family of Anthrax Victim.” *Baltimore Sun*. <http://www.ph.ucla.edu/epi/bioter/hospitalsued.html> (accessed March 1, 2006).
- McNeil, Donald G. and Lawrence K. Altman. “As SARS Outbreak Took Shape, Health Agency Took Fast Action.” *The New York Times*, Section 1, Column 1, Foreign Desk, May 4, 2003. <http://query.nytimes.com/gst/fullpage.html?sec=health&res=9A0CE2D7123CF937A35756C0A9659C8B63> (accessed November 30, 2006).
- Miller, Judith, Stephen Engelberg, and William Broad. *Germs: Biological Weapons and America's Secret War*. New York, NY: Simon and Schuster, 2001.
- Monke, Jim. *Agroterrorism: Threats and Preparedness*. Washington, D.C.: Congressional Research Service, August 25, 2006. <http://www.nationalaglawcenter.org/assets/crs/RL32521.pdf#search=%22Agroterrorism%3A%20Threats%20and%20Preparedness%202006%22> (accessed October 5, 2006).
- National Broadcast Corporation. “Feds: New Safety Plan Required before Spinach is Sold: E. Coli Source Discovered in Refrigerator.” NBC11.com. <http://www.nbc11.com/news/9903292/detail.html> (accessed September 27, 2006).
- National Defense University. *Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks*. Washington, D.C.: Center for Counterproliferation Research, November 2002. http://www.ndu.edu/centercounter/prolif_publications.htm (accessed November 26, 2005).

- . *Toward a National Biodefense Strategy: Challenges and Opportunities*. Washington, D.C: Center for Counterproliferation Research, 2003.
<http://www.ndu.edu/centercounter/CCR%202003.pdf> (accessed December 20, 2005).
- National Journal Group. “Inconclusive Test Results Cited in Delayed Tularemia Notification to Federal, Local Health Agencies.” Global Security Newswire.
http://www.nti.org/d_newswire/issues/2005/10/5/35653f39-93ee-416f-9540-a8cc79aaf652.html (accessed December 20, 2005).
- National Response Team. *Observations and Lessons Learned from Anthrax Response: National Response Team Interim Report [Draft]—October to November, 2001*.
[http://www.nrt.org/production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/A-80anthrax/\\$File/ANTHRAX_Report_07_13_04.pdf?OpenElement](http://www.nrt.org/production/NRT/NRTWeb.nsf/AllAttachmentsByTitle/A-80anthrax/$File/ANTHRAX_Report_07_13_04.pdf?OpenElement) (accessed November 26, 2005).
- Parachini, John. *Anthrax Attacks, Biological Terrorism and Preventive Responses*. Santa Monica, CA: RAND Corporation, 2001.
<http://www.rand.org/publications/CT/CT186/> (accessed October 15, 2006).
- Parker, Henry S. “Agricultural Bioterrorism: A Federal Strategy to Meet the Threat.” *McNair Paper* no. 65 (March 2002).
<http://www.au.af.mil/au/awc/awcgate/ndu/mcnair65.pdf> (accessed November 26, 2005).
- Partnership for Public Service. “Homeland Insecurity: Building the Expertise to Defend America from Bioterrorism.”
http://www.ourpublicservice.org/research/research_show.htm?doc_id=181630 (accessed November 26, 2006).
- Shaughnessy, Larry. “Navy Tests Entire USS Reagan Crew for Tuberculosis.” CNN.com.
<http://www.cnn.com/CNN/Programs/situation.room/blog/2006/07/navy-tests-entire-uss-reagan-crew-for.html> (accessed September 27, 2006).
- Shea, Dana A. and Frank Gottron. *Small-Scale Terrorist Attacks using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons*. Washington, D.C.: Congressional Research Service, May 20, 2004.
<http://fpc.state.gov/documents/organization/33629.pdf> (accessed March 28, 2006).
- Shea, Dana A. *The National Biodefense Analysis and Countermeasures Center: Issues for Congress*. Washington, D.C.: Congressional Research Service, October 4, 2006.
- Stern, Jessica. “Confronting Biological Terrorism: Global Epidemiological Monitoring.” *Harvard International Review* 23, no. 1 (2001). <http://hir.harvard.edu/articles/1008/> (accessed October 15, 2006).

- . “Terrorist Motivations and Unconventional Weapons.” Chap. 8 in *Planning the Unthinkable: How New Powers Will use Nuclear, Biological, and Chemical Weapons*. Edited by Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz. Ithaca, NY: Cornell University Press, 2000.
- The New York Times*. “Former Aides to Guru in Oregon Plead Guilty to Numerous Crimes.” http://topics.nytimes.com/top/reference/timestopics/subjects/i/immigration_and_refugees/index.html?query=ONANG,%20DIANNE%20Y&field=perandmatch=exact (accessed September 20, 2006).
- The White House. *National Strategy for Combating Terrorism*. Washington, DC: The White House, September 2006. <http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf> (accessed September 20, 2006).
- . *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: The White House, February 2003. http://www.whitehouse.gov/pcipb/physical_strategy.pdf (accessed September 20, 2006).
- Thompson, Christopher M. “The Bioterrorism Threat by Non-State Actors: Hype or Horror?” Masters thesis, Naval Postgraduate School, December 2006.
- Thompson, Marilyn W. *The Killer Strain: Anthrax and a Government Exposed*. First ed. New York: Harper Collins, 2003.
- Török, Thomas J., R. V. Tauxe, R. P. Wise, J. R. Livengood, R. Sokolow, S. Mauvais, K. A. Birkness, M. R. Skeels, J. M. Horan and L. R. Foster. “A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars.” In *Biological Weapons: Limiting the Threat*, edited by Joshua Lederberg, 167-184. Cambridge, MA: MIT Press, 1999.
- Tucker, Jonathan B. “Historical Trends Related to Bioterrorism: An Empirical Analysis.” *Emerging Infectious Disease* 5, no. 4 (July/August 1999), <http://www.cdc.gov/ncidod/EID/vol5no4/pdf/tucker.pdf> (accessed September 20, 2006).
- . “Introduction.” Chap. 1 in *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. Edited by Jonathan B. Tucker. Cambridge, MA: MIT Press, 2000.
- UCLA Department of Epidemiology, School of Public Health. “American Anthrax Outbreak of 2001.” http://www.ph.ucla.edu/epi/bioter/detect/antdetect_intro.html (accessed March 1, 2006).
- United States Government. *CONPLAN: United States Government Interagency Domestic Terrorism Concept of Operations Plan*. Washington, D.C.: United States, 2001.

- Wagner, Michael M., Virginia Dato, Michael P. Allswede, Ron Aryel, and Abi Fapohunda. *The Nation's Current Capacity for the Early Detection of Public Health Threats Including Bioterrorism*. Rockville, MD: Agency for Healthcare Research and Quality, September 26, 2001.
<http://rods.health.pitt.edu/LIBRARY/dato1AHRQInterimRpt112601.pdf> (accessed March 29, 2006).
- Warrick, Joby. "Tight lid kept on new U.S. bioterror facility." *The Seattle Times*, August 1, 2006.
http://seattletimes.nwsources.com/html/nationworld/2003166525_bioterror01.html (accessed November 26, 2006).
- Widdowson, Marc-Alain, Arnold Bosman, Edward van Straten, Mark Tinga, Sandra Chaves, Liesbeth van Eerden, and Wilfred van Pel. "Automated, Laboratory-Based System using the Internet for Disease Outbreak Detection, the Netherlands." *Emerging Infectious Diseases* 9, no. 9 (August 12, 2003),
<http://www.cdc.gov/ncidod/EID/vol9no9/02-0450.htm> (accessed October 15, 2006).
- Wilson, William L. "Biological Warfare Defense. 1. Introductory Remarks," *American Journal of Public Health* 42, no. 3 (March 1952): 233-4.
- Woods, Jon B. *USAMRIID's Medical Management of Biological Casualties Handbook*. Sixth ed. Fort Detrick, MD: USAMRIID, April 2005.
<http://www.usamriid.army.mil/education/bluebookpdf/USAMRIID%20BlueBook%206th%20Edition%20-%20Sep%202006.pdf> (accessed October 25, 2006).
- Zilinskas, Raymond A. "Biocriminality and Bioterrorism: Assessing the Threats." Presentation given as part of Workshop 548, Simulating a Deliberately Caused Foodborne Disease Outbreak Using the Table-top Exercise (TTX), at Monterey Institute of International Studies on 4 and 12 November 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, VA
2. Dudley Knox Library
Naval Postgraduate School
Monterey, CA
3. Department of Homeland Security
Directorate for Preparedness
Washington, DC
4. Department of Homeland Security
Management Directorate
Washington, DC
5. Department of Homeland Security
Office of Policy Directorate
Washington, DC
6. Department of Homeland Security
Office of Operations Coordination
Washington, DC
7. Department of Homeland Security
Federal Law Enforcement Training Center
Washington, DC
8. Centers for Disease Control and Prevention
Coordinating Office for Terrorism Preparedness and Emergency Response
Atlanta, GA
9. U.S. Pacific Command
Directorate of Plans and Policy
Weapons of Mass Destruction, Homeland Defense, and Functional Plans Division
(PACOM/J574)
Camp H.M. Smith, HI
10. Peter R. Lavoy
Department of National Security Affairs, Center for Contemporary Conflict
Naval Postgraduate School
Monterey, CA

11. Anne L. Clunan
Department of National Security Affairs, Center for Contemporary Conflict
Naval Postgraduate School
Monterey, CA
12. Craig Hooper
Center for Nonproliferation Studies
Monterey Institute of International Studies
Monterey, CA
13. Raymond Zilinskas
Center for Nonproliferation Studies
Monterey Institute of International Studies
Monterey, CA
14. Cindy Lambdin
U.C. Berkeley Center for Infectious Disease Preparedness, School of Public
Health
Berkeley, CA
15. David Sullivan
City and County of San Francisco, Office of Emergency Services and Homeland
Security
San Francisco, CA
16. Major Christopher M. Thompson
Department of National Security Affairs
Naval Postgraduate School
Monterey, CA